UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT

UNCTAD

Study on prospects for harmonizing cyberlegislation in Central America and the Caribbean

UNITED NATIONS

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT

STUDY ON PROSPECTS FOR HARMONIZING CYBERLEGISLATION IN CENTRAL AMERICA AND THE CARIBBEAN

UNITED NATIONS
New York and Geneva, 2011

NOTE

United Nations documents are designated by combinations of uppercase letters and numbers. Where such designations appear, they refer to United Nations documents.

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

UNCTAD/DTL/STICT/2009/3

A UNITED NATIONS PUBLICATION

ACKNOWLEDGMENTS

This study was prepared as part of the work that the UNCTAD Science and Technology and Information and Communication Technology Branch, Division of Technology and Logistics, and the TrainForTrade Programme have been conducting since 2007 to create competencies in the area of cyberlegislation.

Mr. Jorge Navarro Isla served as principal consultant for the study. However, we would also like to thank the participants of the Regional Workshop on Cyberlegislation, held in El Salvador in 2008 for their important contributions. They are: Walter Delangton Villavicencio, Natalia Porras Zamora, Gustavo Guillén Picado, Aura Lizeth Barahona Jácome, Zulma Maite Ávila Herrera, César Adrián Estrada Duque, Ana Josefa Ramírez Hernández, Doris Alicia Madrid Lezama, Elena María Freije Murillo, Richard Francisco Oviedo Mayorga, Armin Adariel Santamaría Cano, Xalteva Izayana Mercado Áreas, Lilian Marie Norato Solís, Jorge Alejandro Troyano Carracedo, Edwin Kadir González Alemany, Blas Minaya Nolasco, Carmen Elena Castillo Gallandat, Marjorie Chorro de Chávez, Ana Yesenia Granillo de Tobar, Tania Isabel Barrera Quintanilla, Gilberto Antonio Lara Sosa, José Ricardo Ramos Sosa, Sigfredo Armando Figueroa Salinas, Julio Alexander Castro, Ricardo Augusto Cevallos Cortez, Alberto Santos Mejía Hernández and Ana Tomasino.

Important contributions were also made by Sócrates Elías Martínez de Moya, Luca Castellani (UNCITRAL), Cécile Barayre, Gonzalo Ayala and Solange Behoteguy.

PREFACE

The deployment of information and communication technologies (ICT) has radically changed the business environment in developing countries. These technologies create new development opportunities, help attract foreign direct investment, and permit small and medium-sized enterprises to participate more actively in international trade and in reducing the various manifestations of the digital gap.

Such benefits, however, are not automatic. The role of government is paramount in stimulating the use of ICT and establishing appropriate legal frameworks for the development of electronic commerce (e-commerce) and electronic government (e-government) services. The existence of legal frameworks ensures trust between trade partners, facilitates domestic and international trade and provides legal protection for users and providers of e-commerce services. In this context, it is important work towards harmonizing the legislation of the various countries.

Since 2007, UNCTAD, with support from the Kingdom of Spain, has been involved in various activities to help strengthen human resource capacities in public administration and in the private sectors of countries that are members of the Latin American Integration Association (ALADI), as well as in the Central American and Caribbean countries. It supports government efforts to understand the legal complexities involved in ICT and to create national and regional legal frameworks to provide for international harmonization. In June 2009, UNCTAD published a study on prospects for harmonizing cyberlegislation in Latin America (UNCTAD/DTL/STICT/2009/1).

The present "Study on prospects for harmonizing cyberlegislation in Central America and the Caribbean" was undertaken to fill the need of the region's countries for more material for developing normative frameworks and facilitating e-commerce. Its conclusions offer suggestions for potential agreement on harmonized regulatory strategies that are in line with contemplated regional commitments, such as those involved in eLAC 2007 and eLAC 2010, as well as with international instruments such as the United Nations United Nations Convention on the Use of Electronic Communications in International Contracts, which was developed by the United Nations Commission on International Trade Law (UNCITRAL). The aim is to harmonize the countries' normative frameworks and public policies in a complex regulatory context of diverse legal provisions and programmatic instruments at the regional, national and international levels. The study focuses particularly on legislation affecting electronic transactions and electronic signature, electronic contracts, consumer protection, the privacy and protection of personal data, cybercrime, intellectual property and domain names.

The study approaches the situation of each Central American and Caribbean country in both the regional and Latin American contexts. Thus, it can be useful to government personnel designing and implementing legal frameworks to foster development.

CONTENTS

I. BACKGROUND

As part of its work in Latin America, and with a view to expanding its activities in the region, UNCTAD organized launched its first distance-learning course, "Legal Aspects of Electronic Commerce", which took place from 19 January to 13 February 2009. Ninety delegates from different Central American and Caribbean countries participated, representing Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua, Panama and the Dominican Republic.

Subsequently, a "Regional Workshop on Cyberlegislation" was held from March 23 to 27 2009 in San Salvador, with 26 delegates selected from among the participants in the online course. The objectives of the workshop were to further knowledge of cyberlegislation, share different countries' regulatory experiences and encourage the development of a multidisciplinary working group specializing on the legal aspects of e-commerce.

The present study is based on the findings of the "Study on prospects for harmonizing cyberlegislation in Latin America" and on the normative materials prepared for the participants of the San Salvador workshop, including questionnaires that UNCTAD provided on laws and regulations, delegates' preliminary reports and presentations, and consultation with local and international experts. Legal provisions described on the websites of the major government agencies of the countries represented were also reviewed.

II. NORMATIVE REPORT OF PARTICIPATING COUNTRIES

This section describes normative developments in the region and in each of the participating countries, providing brief descriptions of legislation and regulation on (i) electronic transactions and electronic signature in the commercial and financial realm, as well as in government; (ii) consumer protection; (iii) privacy and data protection; (iv) intellectual property; (v) domain names; (vi) cybercrime; and (vii) taxes and customs.

The level of harmonization of national normative structures varies, since both normative strategies and the laws that have functioned as frames of reference for their creation differ considerably from country to country. This is clear for each area of the study. However, it is clearest in relation to e-commerce, where Panama and the Dominican Republic have adopted special laws, while Costa Rica, El Salvador, Guatemala, Honduras and Nicaragua bring to bear laws originally designed for other purposes.

The international regulatory scene and, in particular, that of the region, reflect important advances in legislative and regulatory harmonization, especially with regard to e-commerce, foreign trade and intellectual property. This is a result of the signing and adoption of the United States-Central America-Dominican Republic Free Trade Agreement (CAFTA-DR) and of the existence of the Unified Central American Customs Code (CAUCA) and the regulations associated with it (RECAUCA), which incorporate regulatory provisions consistent with international best practices to encourage the development of e-commerce, and which have motivated the countries to review their domestic regulations and update them in accordance with these treaties.

(A) Costa Rica

Costa Rica has no specific legislation regulating e-commerce. However, there are legal provisions in various areas that affect certain aspects of e-commerce. Among the most important are the Digital Certificates, Digital Signature and Electronic Documents Act (Law 8454), the Civil Code (Law 63), the Commercial Code (Law 3284) and the Promotion of Competition and Effective Consumer Protection Act (Law 7472).

1. Electronic transactions and electronic signatures

The Digital Certificates, Digital Signature and Electronic Documents Act (Law 8454) incorporates certain principles from the UNCITRAL Model Law on Electronic Signatures,[1] and establishes a general legal framework for the transparent, reliable and secure use of electronic documents and electronic signature by public and private entities that:

- 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; and
- explicitly authorizes the State and all public entities to use digital certificates, digital signatures and electronic documents in their areas of authority.

The guiding principles of this law include: (i) minimal legal regulation and formalities, deregulation; (ii) shaping of relationships between private parties according to the autonomous will of the parties; and (iii) equal treatment for different technologies used to create, process and store information.

The law also recognizes the probative value and functional equivalency of printed documents and electronic or digital ones, as well as of documents with handwritten signatures and those with digital signatures. The law provides that electronic documents may be used for: (i) the formation, formalization and execution of contracts; (ii) legal notifications; (iii) the processing, handling and archiving of judicial and administrative files; (iv) the issuance of certificates, affidavits and other documents; (v) the submission, processing and registration of documents in the National Register; and (vi) the handling, preservation and use of notarial protocols.

The law defines the term "digital signature" as the set of data attached to, or logically associated with, an electronic document that make it possible to verify its integrity, as well as to identify the author unequivocally and to legally link him or her with the electronic document. It also provides that a "digital signature" is "certified" if it is issued under a digital certificate that is in force and has been issued by a registered certification entity. Public electronic documents must bear certified digital signatures.

Furthermore, it defines the concept of "digital certificate" as the electronic or digital mechanism that makes it possible to guarantee, confirm or technically validate: (i) the legal link associating a document, a digital signature and a person; (ii) the integrity, authenticity and general non-altered state of the document, as well as of the digital signature associated with it; and (iii) the authentication or certification of the document and the digital signature associated with it, assuming that publicly granted powers of certification have been employed.

The law authorizes certifiers of signatures to issue digital certificates, and grants authority to the Digital Signature Certification Direction of the Ministry of Science and Technology to administer and oversee the certification system. It also indicates the causes for which digital certifications may be suspended or revoked, and defines cases in which digital certificates issued abroad are considered to have full legal value and force.

a. Commerce and finance

With regard to electronic transactions in commerce, the Commercial Code (Law 3284), which governs acts of commerce, does not explicitly regulate electronic contracts. However, offers made by means of websites are deemed to be subject to the provisions of article 445, which establishes that public solicitations in the form of circulars, advertisements and other media used by merchants do not obligate the merchants to any specific person, but only to the first person to accept an offering.

[1] www.uncitral.org

By virtue of a provision of the Commercial Code, the Civil Code (Law 63) functions as an additional source of regulations applying to various matters not covered by the Commercial Code. Thus, provisions on contract formation and required contract formalities are applicable in the digital domain. The norms governing offerings to the public and acceptance thereof, formation of contracts between present parties and absent parties, and the time and place at which a contract is executed also apply.

Article 632 of the Commercial Code establishes an important precedent for facilitating commerce, by allowing banks, at the request of a client, to certify via microfilm, digital image or electronic file, images of checks that clients have written against their checking accounts. It furthermore establishes as the maximum period for requesting such certification four years from the date on which the check is paid. Microfilm or certified digital imagery of documents concerned with checking account operations are deemed full evidence with respect to the original document, and have the same legal value as the original. Article 632 authorizes the Central Bank of Costa Rica to determine through regulation of the settlement system the conditions that certified digital images must meet.

b. Government

As regards public contracting, the Administrative Contracting Act (Law 7494) provides a basis for incorporating the use of electronic communications in the contracting process. Article 40 of the law states that:

- To communicate procedural actions, the government may use any electronic medium that provides certainty of receipt and that ensures message content.
- When the efficiency of contracting procedures so demands, the government may require bidders and entities appearing on registries of providers to indicate e-mail addresses, fax numbers or telematic information for official communications.
- This law also mandates that regulations may define the conditions for the transmission of bids and clarifications sent to the government through the above-mentioned electronic media.

The Regulations for the Use of the Government Procurement System, CompraRED -Executive Decree 32717, complements Law 7494, and explains that the object of CompraRED is to promote the transparency, efficiency, efficacy and regional and global integration of the Costa Rican State's procurement process. The system makes it possible to electronically publish requests for goods, works and services; to provide information on the procurement process from beginning to end, including decisions on, and results of, purchases; and allow potential providers, citizens and the government itself to obtain relevant information online.

Based on Law 8454, the executive branch issued the Regulations for the Electronic Certificates, Digital Signature and Electronic Documents Act (Decree 33018), which govern the operational aspects of the certification system in more detail and cover, among other things, various types of public key infrastructure (PKI). Also relevant is Executive Decree 35139, which creates the Inter-Agency Commission on Digital Government, a coordinating body responsible for defining public policy on digital government.

2. Consumer protection

Addressing consumer protection, the Promotion of Competition and Effective Consumer Protection Act (Law 7472) incorporates the basic principles of consumer relations set forth in United Nations General Assembly Resolution 39/248, which concerns the Consumer Protection Guidelines. Law 7472 deals with a variety of elements appearing in the regulations of different countries such as Germany, Argentina, Brazil, Chile, Spain, United States, Mexico and Venezuela.

Among other things, Law 7472 regulates merchants' obligations to consumers. Article 31 of the law establishes that all information, advertising or public offering of goods or services in any medium or form of communication is binding on the producer transmitting it, using it or ordering its dissemination, and is a part of the contract.

In addition, article 29 enshrines a number of fundamental and inalienable consumer rights: (i) protection against risks that could jeopardize their health or security, or that of the environment; (ii) protection of their legitimate economic and social interests; (iii) access to accurate and timely information on the different goods and services, with accurate specification of quantity, characteristics, composition, quality and price;

(iv) education and disclosure regarding the proper use of goods or services, to ensure free choice and equitable contracts; (v) administrative and judicial protection against misleading advertising, and against abusive practices and clauses, as well as against unfair commercial methods or those that limit the freedom of choice; (vi) effective mechanisms to obtain administrative and judicial protection of consumers' rights and legitimate interests, and to ensure adequate prevention, sanctions and prompt compensation for violations, as appropriate; (vii) State support for the creation of consumer groups and organizations, and opportunities for their points of view to be heard regarding decisions that affect them. The above-mentioned article makes no distinction as to mode of transaction; thus these rights apply to both traditional operations and operations carried out in a digital environment.

Article 39 is also important. It prohibits and declares null and void any abusive clauses in adhesion contracts. Clauses of such contracts are deemed abusive if they: (i) restrict the consumer's rights without making this clear in the text of the clauses; (ii) limit or eliminate the provider's (merchant's) obligation; (iii) excessively or disproportionately favour the contractual position of the provider, or imply a waiver or restriction of the consumer's rights; (iv) relieve or limit the liability of the provider for bodily harm, and for defective compliance or delayed delivery; (v) permit the provider to unilaterally annul the contract, change its conditions, suspend its execution, or revoke or limit any of the member's rights under the contract, except when such annulment, change, suspension, revocation or limitation is the result of the consumer's failure to meet obligations; (vi) obligate the consumer to waive in advance any right under the contract; (vii) entail the consumer's waiver of procedural rights enshrined in the Code of Civil Procedure or in special laws related to it; (viii) are illegible; or (ix) are written in a language other than Spanish.

Article 39 declares null general clauses of adhesion contracts that: (i) give the provider a disproportionate or imprecise period of time for accepting or rejecting a proposal or for performing a service; (ii) give the provider a disproportionate or insufficiently precise time for providing a service that it is obligated to provide; (iii) obligate the consumer to manifest his/her will on the basis of presumed knowledge of other legislative or regulatory provisions that are not an integral part of the contract; (iv) provide for disproportionate claims, penalties or interest in connection with damages to compensate a consumer; or (v) fail to indicate payment conditions, annual interest rates, late fees and interest, commissions, surcharges, additional charges, and other conditions that are binding on the user if he/she signs the contract.

Article 39 also provides that the legal validity of the general conditions of an adhesion contract, modifications to it, annexes or addenda, be actually known to the consumer, or knowable to the consumer through ordinary acts of diligence. It also establishes that ambiguous general conditions shall be interpreted in favour of the consumer.

Article 60 sanctions as a crime against the consumer that of "fraud" by a party committed to delivering a good or performing a service that is offered publicly, as defined in articles 31 (merchant's obligations), 34 (offerings, promotion and advertising) and 38 (promotions and special offers), if the good or service is not provided pursuant to the agreed conditions, in a manner that involves some misleading or otherwise manipulative action. The National Consumers' Commission is empowered to refer such cases to the criminal justice system.

3. Privacy and data protection

With regard to privacy and data protection legislation and regulations, the individual rights enshrined in article 24 of the Costa Rican Constitution include the right to privacy, freedom and confidential communications. Under this article, the private documents of the country's inhabitants, as well as their written, oral and all other types of communications, are inviolable. However, the courts can order the seizure, search or examination of private documents when this is essential for clarifying matters before them. It also defines the cases in which the courts may order the interception of any type of communication, and indicates the crimes in which investigation this exceptional authority can be exercised, and for how long it can take place.

On the international front, Costa Rica has adopted the Universal Declaration of Human Rights and the Inter-American Convention on Human Rights, or San José Pact, which recognize as fundamental rights the right to confidentiality and to a private life.

In the national context, the General Telecommunications Act (Law 8642) includes a number of measures protecting the privacy, rights and interests of the end users of telecommunications services. As a frame of

reference, it takes the European Council Directive CE 2002/58 (Directive on privacy and electronic communications), which covers the treatment of personal information and privacy protections in the electronic communications sector.

Under this law, operators of public networks and providers of telecommunications services available to the public must guarantee the confidentiality of communications, the privacy, and protection of the personal information of subscribers and end users. It also requires operators and providers to guarantee that communications and the traffic data associated with them will not be listened to, recorded, stored, intercepted or monitored by third parties without consent, except with due judicial authorization pursuant to the law.

It also creates an explicit prohibition on using automatic voice, fax, e-mail or other calling systems for direct marketing, except in the case of subscribers who have previously consented to such use. However, when a natural or juridical person obtains a client's e-mail address with the latter's consent, in the context of the sale of a product or service, said person is permitted to use this information for direct marketing of other similar products or services that he/she/it provides.

The law also prohibits sending electronic messages for direct marketing purposes when the identity of the sender is disguised or hidden, or when a valid address is not provided in order to allow the addressee to request an end to such communication.

The Insurance Market Regulation Act (Law 8635) and the Credit Card Regulation Act (Decree 28712) also contain measures to protect the personal information of users of the services that they regulate.

4. Intellectual property

In the area of intellectual property, the Copyright and Related Rights Act (Law 6683) protects artistic and literary works, as well as computer programs and databases – as compilations. It also defines any permanent or temporary electronic storage of a copy of a literary or artistic work as a reproduction. In connection with the related rights of artists, performers, producers of phonograms and broadcast entities, the law defines the concepts of phonograms and videograms, and recognizes the right of public communication via any medium.

The Regulations of the Copyright and Related Rights Act (Decree 24611) expands the act's catalogue of definitions. A relevant definition is the provided for "broadcast or transmission", which is defined as the communication of works, sounds or sounds with images via radio waves, cable, fibre optic cable and similar procedures, whether in real time or not. The definition also include signals sent from a terrestrial station to a satellite that subsequently retransmit it.

In the area of industrial property, the Patents, Drawings and Industrial Models Act (Law 6867) does not cover mathematical methods or computer programs in isolation as inventions subject to patenting, and the Undisclosed Information Act (Law 7975) and the associated regulations (Decree 34927) protect trade and industrial secrets held confidentially by a natural or juridical person, in order to prevent information legitimately under his/her/its control from being disclosed to third parties, or from being acquired or used by third parties without his/her/its consent in a way inconsistent with honest commercial use.

The Trademarks and Other Distinguishing Marks Act (Law 7978) establishes requirements and terms governing the protection of trademarks, trade names, denominations of origin and other distinguishing signs. It defines the conditions under which a brand is deemed to be in use, but does not explicitly cover the use of the brand on the Internet. The Procedures of Observance of Intellectual Property Rights Act (Law 8039) governs administrative and judicial action to combat violations of intellectual property rights, including, among others, precautionary measures and border measures. It also defines the authority of the Administrative Registry Tribunal to resolve conflicts in this area.

In the context of international intellectual property rights, Costa Rica has ratified:

- The WIPO Copyright Treaty (WCT) and Performances and Phonograms Treaty (WPPT);
- The Protocol to the Central American Agreement for the Protection of Industrial Property
- The United States-Central America-Dominican Republic Free Trade Agreement

- The Lisbon Agreement for the Protection of Designation of Origin and their International Registration
- The Paris Convention for the Protection of Industrial Property (1883)
- The Berne Convention for the Protection of Literary and Artistic Works
- The Geneva Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of their Phonograms
- The Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations
- The 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 the World Trade Organization (WTO).

5. Domain names

With regard to domain names, the National Academy of Sciences, through its subsidiary NIC-Internet Costa Rica (http://nic.cr), is responsible for administering and coordinating the functioning 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 so ordered by a domestic or foreign court. In the latter case, the party to whom the judgement applies must follow a procedure for the recognition of foreign judgements in Costa Rica.

NIC-Internet Costa Rica proceeds to remove the domain name once it receives written notification by the domestic or international court with the recognition-of-judgement, if relevant. Once the domain name is removed, NIC-CR sends an automatic electronic notice to the e-mail addresses of the domain name's contacts, informing them of the removal. The procedure does not conform to the Uniform Domain-Name Dispute-Resolution Policy of the Internet Corporation for Assigned Names and Numbers (ICANN).

6. Cybercrime

The Penal Code provides for prison sanctions for: (i) persons who take control of, gain access to, modify, alter, delete, intercept, interfere with, use, disseminate or deflect 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) persons who influence 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) persons who by any unauthorized means access, erase, delete, modify or render unusable data recorded in a computer.

7. Taxes and customs

The General Customs Act (Law 7557) provides for prison sanctions of one to three years for: (i) persons who by any unauthorized means access computer systems used by the National Customs Service; (ii) persons who, without customs authority, take control of, copy, destroy, render unusable, alter, facilitate the transfer of or possess any computer program used by the National Customs Service, or its data bases, provided that said Service has declared them to be of restricted use; (iii) persons damaging the material or physical components of devices, machines or accessories that support the functioning of the computer systems designed for the operations of the National Customs Service in order to obstruct their functioning or obtain benefit for his/herself or for a third party; or (iv) persons who improperly facilitate use of the username and password assigned for entry to the computer systems.

The Information Technology for the Customs Control (TICA) system was created under various amendments to the General Customs Act (Law 7557) and the associated Regulation 34475-H and the related guidelines. It provides, among other things, for electronic handling of customs declarations and other related procedures. This measure meets obligations under the free trade agreements signed by Costa Rica and under other legal instruments described in the paragraphs below.

A single window for foreign trade has also been created with the support of different laws, such as the Law 7638 and the Law to Protect Citizens from Excessive Administrative Requirements and Procedures (Law 8220), which, among other things, stipulates that a government entity, organ or official to which/whom information is submitted by an administrative body may not require that the same information be submitted anew to the same entity, organ or official in connection with the same proceeding or with any other proceeding of that same entity or body. This law mandates that information must be obtained in a coordinated manner.

As regards international treaties dealing with e-commerce and electronic transactions, the United States-Central America-Dominican Republic Free Trade Agreement (CAFTA-DR), the Canada-Costa Rica Free Trade Agreement and the Unified Central American Customs Code Regulations are remarkable instruments. Given their regional importance, these are described in more detail below.

Chapter V.- Customs Procedures of the Canada-Costa Rica Free Trade Agreement, consistent with the above-mentioned treaties, establishes various measures to facilitate trade by incorporating electronic media. In particular, section 8 of article IX.2.- Specific Obligations Under the Treaty - requires the parties to work towards common processes and to simplify the information needed to clear merchandise, and to apply current international norms where appropriate. For this purpose, the parties are obligated to create the means of providing for electronic data exchange between customs administrations and the trade community in order to promote expedited clearance procedures.

For the purposes of article IX.2, the parties are to use formats based on international electronic data exchange standards, and to take into account the recommendations of the World Customs Organization related to "the use of the UN/EDIFACT rules for electronic data interchange" and to "the use of codes for the representation of data elements", without prejudice to the use of additional standards for electronic data transmission.

Article IX.3 of the Treaty- Cooperation - obligates the parties to recognize that technical cooperation is an essential element of facilitating compliance with the treaty's obligations. To further facilitate trade, the parties agree to collaborate in strengthening their own measures for cooperation within their individual customs administrations so as to promote cooperation in areas such as electronic data exchange. Moreover, the two countries' Joint Statement on Electronic Commerce recognizes the importance of online trade mechanisms to foster the economic development in both countries.

8. Legislative initiatives

Among the main legislative initiatives and regulatory proposals that deserve a special mention are the following:

(i) Legislative bill 16081, which aims to provide regulation of the legal regime governing services contracted and provided via the Internet;

(ii) Regulations on Measures to Protect the Privacy of Communications, which are set forth in the General Telecommunications Act, title II, chapter II, with various measures to protect personal information in electronic communications;

(iii) Legislative bill 16.546, which proposes to add new articles to the Penal Code expanding the list of cybercrimes, including, among others, the swindle by means of credit or debit card, computer fraud with debit/credit cards, national fraud, industrial and individual fraud;

(iv) Legislative bill 17164, which contains proposed legislation to protect children and adolescents from harmful content on the Internet and in other electronic media.

In the international context, and particularly in the context of regulatory harmonization promoted by CAFTA-DR, the Government of Costa Rica is in the process of reviewing and analysing the United Nations Convention on the Use of Electronic Communications in International Contracts (CUECIC), with a view to the possibility of signing it.

(B) Dominican Republic

The Dominican Republic has adopted a special law on e-commerce, and has modified its tax laws to include the use of electronic media in relation to various tax procedures and obligations.

1. Electronic transactions and electronic signature

Law 126-02 on e-commerce, documents and digital signature incorporates various principles of the UNCITRAL Model Law on Electronic Commerce. According to article 1, this law applies to all types of information in the form of digital documents or data messages, except where other legal provisions require printed information, or in the context of obligations that the Dominican State has under international agreements or treaties.

Article 56 of the law authorizes the Dominican Telecommunications Institute (INDOTEL) to oversee and monitor the activities of certification entities. However, under article 35, regulation and oversight of financial entities is left to the Monetary Board and the Superintendency of Banks.

Article 2 of Law 126-02 defines a number of terms, including e-commerce, which is defined as including all relations of a commercial nature, whether or not contractual, that are based on the use of one or more digital documents or data messages, or other similar media. Commercial relations include, but are not limited to, the following operations:

(i) any commercial operation to supply or exchange goods, services or information;
(ii) any distribution agreement;
(iii) any commercial representation or order;
(iv) purchase of accounts receivable at a discount (factoring);
(v) leasing operations;
(vi) construction of works;
(vii) consulting operations;
(viii) engineering operations;
(ix) granting of licenses;
(x) investment operations;
(xi) financing operations;
(xii) banking operations;
(xiii) insurance operations;
(xiv) any concession agreement or commercial provision of a public service;
(xv) joint ventures and other forms of industrial and commercial cooperation;
(xvi) transport of merchandise or passengers by air, maritime transportation, rail or road.

The law also defines certification entities as institutions or juridical persons that, under the law, are authorized to issue certificates relating to the digital signatures of persons, to offer or provide services that record and stamp data messages as sent or received, or to carry out functions involving communications based on digital signatures.

Article 3 of Law 126-02 sets forth general principles, including the importance of promoting uniform enforcement of the law and observing good faith**,** as well as facilitating commerce and providing for the validity of transactions between parties through new information technologies. The article also recognizes the legal validity of information contained in digital documents and data messages.

Article 5 stipulates that when any legal provision requires information to be in written form, the requirement can be met by a digital document or data message if the information it contains is accessible for later viewing, and if the document or message meets all legal requirements for validity.

Under article 9, digital documents and data messages are admissible as evidence and have the same probative value as that which the Civil Code and Code of Civil Procedure stipulate for signed paper documents. With regard to the probative weight of digital documents or data messages, article 10 stipulates that the reliability of the way in which they have been created, filed or communicated, the reliability of the way in which the integrity of the information has been safeguarded, the way in which the creator or

initiator of the document or message is identified, and any other relevant factors, must be taken into consideration.

In relation to contract formation, article 13 stipulates that, except where the parties have expressly agreed otherwise, an offer and the acceptance of it may be expressed through a digital document, data message, or a data message containing a digital document, as the case may be. A contract's validity or binding quality cannot be denied merely because one or more digital documents or data messages have been used in its formation. Furthermore, article 28 recognizes the legal value of rights conceded or obligations acquired through digital documents or data messages, provided that a reliable method is used to guarantee the uniqueness of said documents or messages.

Article 31 stipulates that the use of a digital signature has the same force and effect as the use of a handwritten one, provided that it meets the following criteria:

(i) it is used by only one person;
(ii) it can be verified;
(iii) it is under the exclusive control of the person who uses it;
(iv) it is linked to the information, digital document or message with which it is associated, in such a way that if the document or message is altered the digital signature is invalidated; and
(v) it meets the criteria of executive branch regulations. Also covered, in article 32, are secure digital signatures, which are those that can be verified in conformity with a system of security procedures that complies with the guidelines set forth in this law and its regulations, as per article 32.

Article 35 establishes the characteristics of and requirements for certification entities, and allows for both public-sector and private-sector, domestic or foreign-based juridical persons, as well as chambers of commerce and production, to function as certification entities once they have requested and received authorization from INDOTEL.

Under article 59, digital certificates issued by foreign certification entities may be recognized, provided that they meet the conditions set forth in the law. In this connection, INDOTEL Board of Directors Resolution 094-04 establishes a procedure for the accreditation of digital signature certification entities in the United States as a way of eliminating the requirement that United States firms that provide signature certification be legally domiciled in Dominican territory.

Article 29 regulates legal instruments related to contracts for the transport of merchandise. Included are regulations on the receipt and shipping of merchandise, and those relating to notifications or statements about the fulfillment of contracts.

a. Commerce and finance

The second paragraph of article 35 of Law 126-02 authorizes the Monetary Board to regulate all matters related to financial operations and services associated with electronic means of payment used in the nation's financial system. It also gives supervisory authority for such matters to the Superintendency of Banks, pursuant to current banking law. In exercising this authority, the Monetary Board issued Payment Systems Regulations, which establish a legal regime applying to the Dominican Republic's payments and settlements system (SIPARD). In addition, it issued Instructions for the Authorization and Operation of Electronic Currency Trading Platforms on 26 December 2005. These include operational procedures and standards for technological platforms.

In addition, Law 183-02, the Monetary and Financial Code, authorizes the Superintendency of Banks to supervise financial intermediation entities, which under article 57 must provide any information that the Superintendency requests via electronic media, the technical requirements for which appear in the relevant regulations.

The special regulations set forth in article 79 authorize the Monetary Board to establish requirements for the admission of evidence in electronic form regarding banking matters and debit and credit card operations, as well any other tangible or electronic payment instrument.

With regard to electronic transactions in the context of securities market operations, article 38 of Law 19-2000, which regulates the securities market, authorizes the Superintendency of Securities to create and maintain a registry covering the securities market and products. The registry, which may be electronic, must contain existing public information on securities, issuers and other participants in the securities market who are subject to this law, pursuant to the provisions established in the corresponding regulations.

b. Government

Article 6 of Law 126-02 has special importance, since it 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 the context of e-government, 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.

Under the second paragraph of article 9, administrative or judicial action may not be taken in a way that acts against the efficacy, validity or binding quality and probative value of any type of information in a digital document or message data merely by virtue of the fact that the information is contained in such a document or message, or because it has not been presented in its original form.

2. Consumer protection

The General Consumer Protection Law, Law 358-05 of 19 September 2005, sets forth basic consumer rights in conformity with United Nations General Assembly Resolution 39/248 of 9 April 1985, which deals with the Consumer Protection Guidelines.

Among other basic rights of consumers or users, Article 33 specifies the following:

(i) protection of life, health and physical safety in the context of consumption or use of goods and services;
(ii) education for the consumption and use of goods and services;
(iii) receipt from providers, via data message, internet, message service, promotional or other similar medium, of accurate, clear, timely, sufficient, verifiable information in Spanish regarding the goods and services being offered, as well as on their prices, characteristics, functioning, quality, origin, type, weight, ingredients and components in order of proportional content, and possible risks, so that consumers are able to choose according to their desires and needs;
(iv) protection of consumers' economic interests in the form of equitable, non-discriminatory and non-abusive treatment by goods and service providers; and
(v) access to the relevant jurisdictional organs for the protection of consumers' rights and legitimate interests via procedures that are of brief duration and available without charge.

As regards e-commerce, article 62 stipulates that in the sale of, or contracting of any type for, goods and/or services that are offered or provided outside of the provider's establishment, or for which a medium such as telephone, television, traditional or electronic mail, digital media or any data message medium, internet, message service, or a promotional or similar medium, is used, the provider is obligated, as the case calls for, to:

(i) inform the consumer, in advance, of price, including taxes, form and date of delivery, shipping cost, 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. In such cases, the provider must clearly establish the timeframe for claims; claims costs are the responsibility of the provider. The provider must offer any additional information required for the use of services that differ from those originally contracted for;
(v) cover shipping costs in case of exchanges or repairs covered by guarantee;

(vi) provide prior notice of delivery of a good or service, and allow a minimum period of 3 days for the consumer to reconsider, prior to delivery; and
(vii) provide for and allow the consumer a minimum trial period of 7 business days for returning the good or suspending the service contract.

In addition, article 81 defines membership contracts and forms as contracts and forms written unilaterally, in advance, by a provider of goods or services, and not subject to substantial changes of terms by the consumer or user should he wish to acquire the product or obtain the service. Such contracts must be approved and registered with the Executive Directorate of Consumer Advocacy.

Article 83 stipulates that, to be valid, any membership contract must be in writing and in Spanish, use characters that are quickly and easily legible, be stated in terms that are clear and understandable to consumers or users, and be explicitly accepted by both consumer and provider.

Paragraph 1 of article 83 stipulates that abusive clauses shall be null and void and without force if, among other things:

(i) they exempt the provider from responsibility for defects or irregularities that affect the usefulness or essential purpose of the product or service, or from liability for damages caused to the consumer or user by such products or services;
(ii) they represent a limitation on or waiver of the rights of consumers and users, or excessively or disproportionately favour providers' rights;
(iii) place the burden of proof on the consumer;
(iv) impose an obligation to rely exclusively on mediation, arbitration or other equivalent and similarly motivated procedure to resolve disputes between consumers/users and providers; or
(v) permit the provider to change the terms and conditions of a contract without prior notice.

Article 88 requires that providers' advertising and promotional activities be truthful, that they not be misleading or produce confusion, and that they involve no form of unfair competition. It also requires that medical products, canned foods, cosmetics, tobacco and alcoholic beverages be authorized for sale by health authorities. Advertising that targets children may not contain information, images, sounds, data or references that are physically, mentally or morally harmful to them.

Article 99 obliges providers to issue and deliver to consumers or users a written or digital document or invoice, based on the medium used for the contract. Said document or invoice must be duly stamped, numbered, dated and signed, and must document the provision of the product or service, as well as the quantity, specifications and price, along with the amount of legally required taxes.

With regard to the liability that a provider may incur by violating this law, article 100 provides for both civil and criminal liability. Article 102 is of special note, since it stipulates that producers, importers, distributors, merchants, providers and all persons involved in producing and marketing goods and services are jointly and severally liable under civil law for compensations for injuries or losses produced by the technology, as well as by inadequate, insufficient or incomplete instructions for the use of their products or services.

3. Privacy and protection of personal information

The Constitution of the Dominican Republic establishes citizens' basic rights and duties, which include freedom of expression, and the integrity and inviolability of correspondence and other private documents.

The General Telecommunications Law (Law 153-98 of 27 May 1998) establishes an obligation to respect the inviolability of telecommunications, and prohibits the use of telecommunications in violation of the law or for the purpose of committing crimes or obstructing justice.

Article 57 of Law 53-07, which deals with high-technology crimes and misdemeanours, targets improprieties involved in investigatory actions by authorized entities. It defines as illegal acts the trafficking in or marketing of data obtained in the course of an investigation, as well as disclosure of the personal or commercial data of a person being investigated, except as an integral part of the investigation, and trafficking in or marketing of same. Articles 377 and 378 of the Penal Code are also relevant in this

connection, as they provide sanctions for the illegal disclosure of information that is subject to professional confidentiality.

Law 200-04, which deals with free access to public information, enshrines, among others, the right to access information contained in governmental records and files, and the right to obtain periodic information on the activities of entities and persons carrying out public functions, provided that said free access is not detrimental to the national security, public order, or to public health or morals**,** a third party's right to privacy and confidentiality, or the right for one's reputation to be respected. The law also protects the right to request, receive and disseminate information on the government, and the freedom to submit questions to entities and persons carrying out public functions, as well as the right to obtain copies of documents that compile such information.

The law establishes limitations and exceptions to the obligation of *sujetos obligados* to disclose information, especially when doing so could be detrimental to the privacy of persons or could jeopardize their lives or safety. The law also stipulates that when access to information depends on the authorization or consent of a third party who is protected by confidentiality rights under the terms of articles 2 and 17 of this law, the information may be provided once the consent of said party is given.

Law 288-05, which created the country's credit information bureaus, deserves special mention. This law protects data concerning the credit histories of physical and juridical persons, and regulates the management, accuracy, veracity and timeliness of the information in the records of the credit information bureaus, while providing sanctions for accessing or disclosing information without the prior consent of the person to whom the information relates.

In addition, section B of article 56 of Law 183-02 mandates banking confidentiality regarding credit operations carried out by the clients of financial intermediation entities. This confidentiality must be maintained, unless otherwise authorized, directly or by the account holder or someone holding power of attorney for such purpose, or by an order of the judicial or tax authorities, or for reasons of preventing money laundering.

In regard to taxation, paragraph IV of article 56 of the Tax Code, amended by Law 495-06 (the Tax Rectification Act), requiring that personal information of taxpayers or parties registered to access the "Virtual Office" and to make tax statements and payments through it be stored in a database that is the property of the Directorate of Internal Revenue (DGII). The information in this database is to be used to correctly identify taxpayers or their representatives who are attempting to access electronically provided services.

Paragraph V of Article 56 of the Code requires the DGII to safeguard the confidentiality of the information supplied electronically by taxpayers or their representatives**,** except when disclosure is necessary to comply with a legal obligation or with an order issued by a duly authorized administrative or judicial entity.

Of note in terms of administrative regulation are the Personal Data Protection Regulations of 23 March 2006, which require certification entities to ensure the protection and confidentiality of information, including personal information, provided by subscribers.

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[2] obligates member countries to guarantee the right to privacy in the handling of personal information.

[2] CARIFORUM includes Antigua and Barbuda, the Bahamas, Barbados, Belize, Dominica, the Dominican Republic, Granada, Guyana, Haiti, Jamaica, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname, and Trinidad and Tobago.

4. Intellectual property

Article 8, section 14 of the Constitution of the Dominican Republic declares that the exclusive ownership of inventions and discoveries, as well as of scientific, artistic and literary productions, are rights of individual persons, for the period and in the manner stipulated by the law.

In this connection, article 2 of Law 20-00 (the Industrial Property Act) states that mathematical methods and computer programs shall not be considered patentable inventions. Article 178 defines business secrets as any undisclosed commercial information that a natural or juridical person possesses that can be used in a productive, industrial or commercial activity, and that can be transmitted to a third party. The article also requires the legitimate owner to take reasonable measures to safeguard the confidentiality of the information.

With regard to industrial secrets, article 179 of Law 20-00 defines the exploitation, communication, disclosure or unauthorized exploitation of such secrets as a form of unfair competition.

The General Law Protecting Consumers' and Users' Rights, Law 358-05, also regulates certain aspects of commercial and industrial secrets subject to confidentiality provisions, defining such secrets as any undisclosed commercial information possessed by a natural or juridical person that can be used in some productive, industrial or commercial activity, and that can be transmitted to a third party. Such secrets are recognized for the purposes of rights protections when the information that constitutes them is not, as a whole or in the precise configuration and combination of components in question in a particular case, generally known or easily accessible to those in circles that normally handle such information, provided that their legitimate owner has taken reasonable measures to maintain their secrecy.

With regard to the use of trademarks, Law 20-00 makes no mention of their use on the internet or in domain names.

As regards copyright, article 2 of Law 65-00, which is devoted to the subject, 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.

Article 169 of the law provides sanctions for various illegal activities, including falsely attributing a work's authorship; altering, eliminating or circumventing technical devices incorporated in protected works, performances, productions, or broadcasts to block or restrict reproduction or control same; and, without authorization, deleting or altering any electronic information regarding collective rights management.

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

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

5. Domain names

With regard to domain names, the Dominican Republic'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 Uniform Domain-Name Dispute-Resolution Policy of the Internet Corporation for Assigned Names and Numbers (ICANN), though they do require parties requesting

registration of a domain name to ascertain that, in doing so, they are not violating any trademark. In cases of disputes between requesters over particular names, the 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.

6. Cybercrime

Law 53-07, the High-Technology Crimes and Misdemeanours Act, includes a number of provisions of the Council of Europe's Convention on Cybercrime, which dates from 23 November 2001. Substantive provisions of this include definitions of crimes involving computer 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.

Article 4 of the law 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. The definition is formulated to include electronic, computer, telematic, cybernetic and telecommunications crimes.

Article 1 also provides for the comprehensive protection of systems that use information and communication technologies, as well as the content of such systems, and the prevention and sanctioning of crimes against them or against any of their components or contents that employ said technologies to the detriment of physical or juridical persons, pursuant to the terms set forth in this law. The integrity of information systems and their components, the information or data that they store or transmit, and commercial or any other type of transaction or agreement concluded through them, as well as the confidentiality of same, are legally protected rights.

The law's scope of application is delimited in article 2, which makes it applicable throughout the territory of the Dominican Republic. It is applicable to any domestic or foreign physical or juridical person perpetrating a prohibited act in any of the following circumstances: (i) when the person committing the act initiates or orders the criminal action within the national territory; (ii) when the person committing the act initiates or orders the criminal action from abroad, producing effects within the national territory; (iii) when the origin or effects of the action occur abroad but employ media located in the national territory; and (iv) when any type of complicity from within the national territory is involved.

Article 4 includes various definitions, including definitions of illicit access, cloning, malicious codes, user data, diverting of contracted facilities, and electronic interception or transfer of funds.

Chapter I, covering crimes and misdemeanours against the confidentiality, integrity and availability of data and information systems, provides sanctions for various crimes relating to: access codes and cloning of access devices; illicit access to electronic, computer, telematic or telecommunications systems or their components; illicit access to provide services to third parties; use of fraudulent devices; intercepting or interfering with data or signals; damaging or altering data; and sabotaging electronic, computer, telematic or telecommunications systems or the programs and logical operations that control them.

Chapter II, Crimes of Content, defines crimes involving actions to jeopardize the life of a person when carried out using electronic, computer, telematic or telecommunications systems or their components; theft that uses high technology; and illicitly obtaining funds through a computerized, electronic, telematic or telecommunications financial service, including electronic funds transfers effected by the illicit use of access codes. Also defined are fraud, blackmail and identity theft committed using high technology; forgery of digital documents, signatures and certificates; use of equipment for the invasion of privacy; illicit commerce in goods and services through the internet; libel and slander committed through electronic, computer, telematic, telecommunications or audiovisual media; and sexual assault and child pornography, including acquisition of the latter through, and intentional possession in, information systems.

Article 25 of chapter III, which covers property crimes and the like, stipulates that when violations, as defined in Law 20-00 of 8 May 2000 on industrial property, and in Law 65-00 of 21 August 2000 on copyright, are committed with the use of electronic, computer, telematic or telecommunications systems or any of their components, the sanctions established in the respective laws on these crimes shall apply.

Chapter IV, Telecommunications Crimes, covers and provides sanctions for fraudulent collect calls, fraud by providers of 1-976-type line information services**,** redirecting of long-distance calls, theft of lines, diverting of traffic, illicit manipulation of telecommunications equipment, and interference with private switchboards.

Chapter V, Crimes Against the Nation and Acts of Terrorism, applies to crimes committed through computer, electronic, telematic or telecommunications systems that: (i) attack basic national interests and security, as in sabotage, espionage and providing of information; and (ii) constitute acts of terrorism.

Chapter I of section II establishes which entities have the authority to investigate and prosecute cybercrimes, with emphasis on the interaction between the Public Ministry and the Department of Telecommunications, Intellectual Property and e-Commerce (a division of the General Prosecutor of the Republic) or any department created for a similar purpose within the prosecutor's office. The chapter also creates and establishes the composition of the Inter-Agency Commission Against High-Technology Crimes and Misdemeanours (CICDAT) and the Department of Investigation of High-Technology Crimes and Misdemeanours (DICAT).

DICAT is the Dominican Republic's official contact point for the International 24/7 Network of Assistance on Crimes Involving High Technology. The network is an offshoot of the Subgroup on High Technology Crimes, which in turn is part of the G8 Group of Experts on Transnational Organized Crime. The law also creates a Cybercrime Investigations Division (DIDI) within the National Department of Investigations.

As regards precautionary and procedural measures, article 52 in chapter II of section II stipulates that the rules on immediate proof and auxiliary media set forth in the Criminal Procedures Code (Law 76-02) apply to obtaining and preserving: data contained in an information system or its components, data traffic, connection data, access data and any other information useful in the investigation of crimes covered by the present law, and for all procedures established in this chapter.

In addition, article 53 requires relevant authorities to act quickly to preserve data contained in an information system or its components, or in a system's data traffic, when data are vulnerable to loss or alteration. Article 54 establishes the areas of authority of the Public Ministry, with the support of DICAT, DIDI, experts and other relevant authorities, to carry out, among others, the following actions:

(i) Order a physical or juridical person to provide the information housed in an information system or in any of its components.
(ii) Order a physical or juridical person to preserve and maintain the integrity of an information system or any of its components for a period of up to 90 days, with this period being extendable for successive periods.
(iii) Access or order access to such an information system or to any of its components.
(iv) Order service providers, including internet service providers, to supply information on user data that may be in their possession or control.
(v) Seize or secure an information system or any of its components in whole or in part.
(vi) Request service providers to collect, extract or record data on a user, such as real time data traffic, using technological tools.
(vii) Access or intercept telecommunications in real time to investigate punishable acts.

Article 56 establishes service providers' obligation to preserve data on traffic, connection and access, or any other information that may be useful for an investigation, for a minimum period of 90 days. It also makes it a duty of the Dominican Telecommunications Institute (INDOTEL) to promulgate regulations regarding service providers' procedures for obtaining and preserving data and information.

7. Taxes and customs

Law 495-06, the Tax Rectification Act, updated a number of articles in the Tax Code of the Dominican Republic to include electronic media as a means of meeting various tax requirements.

Article 2 of the law amends article 44 of the Code by incorporating the authority to store tax-related information in data storage media used in computer systems that process such information, and obligates

taxpayers to permit tax authorities to review such information as part of the oversight function of those authorities.

Article 3 of the law amends article 50 of the Code to permit the orderly preservation, for a 10-year period, of accounting records, special books and records, documents, receipts, or any physical or electronic document relating to the taxpayer's operations and activities.

Article 5 of the law amends article 55 of the Code by incorporating the use of electronic media for personal notifications, which can be made via e-mail, fax or any other electronic means of communication that the Tax Administration agrees upon with the taxpayer. It accords notifications made by e-mail, fax or any other electronic medium the same legal force as those made by constabulary or ministerial means.

The law also authorizes the Tax Administration to make mutual agreements regarding internet addresses or e-mail accounts with taxpayers and their representatives for the purpose of summonses, notifications and other communications related to tax obligations, and for other communications relevant to the taxpayer. When a taxpayer's internet address changes, the taxpayer is required to communicate this to the Tax Administration within the timeframe established in the law.

This law also expands the scope of article 56 of the Code, authorizing taxpayers or those responsible for making tax payments to request the Directorate of Internal Revenue (DGII) to register ID and access codes (PINs) for use in complying with tax obligations by filing sworn statements, sending questions, and settling and paying taxes, as well as for carrying out any other action or service available through electronic media at the internet address provided by DGII for such purposes.

The law authorizes DGII to establish general rules on access, operation, forms of declaration, forms required for tax settlements and payments, as well as all issues relating to the security of the network, timeframes for renewing ID and access codes, and other aspects of the services offered, through electronic media such as the so-called DGII Virtual Office.

Tax statements and updates, made electronically by taxpayers or their representatives at the DGII Virtual Office using ID and access codes previously supplied by DGII, have the same probative value as that accruing to private signed documents under the Civil Code, as established in Law 126-02 of 14 August 2002, which deals with e-commerce and digital signature – provided that the rules established by DGII for the purpose have been followed.

In the area of foreign trade, the Customs Regime Act, Law 3489, makes no reference to electronic media for operations associated with customs clearance. However, Decree 248-09 of 9 July 1998 created the Integrated One-Stop Shop System for Foreign Trade (SIVUCEX), which provides a system of automated electronic procedures for managing all formalities and services needed for export activities.

8. Legislative initiatives.

The roll-out of the E-Dominican Strategic Plan 2007-2010 and the consolidation of the National Commission for the Information and Knowledge Society will be fundamental for developing the regulations to efficiently implement the various laws passed by the country's legislative branch. It should also be noted that a law approving the United Nations Convention on the Use of Electronic Communications in International Contracts (CUECIC) is currently being reviewed in the Senate.

(C) El Salvador

There is no special legislation governing e-commerce in El Salvador, but diverse general laws are applicable. Various provisions of the Civil Code, Commercial Code, Consumer Protection Act, Tax Code and Customs Simplification Act are substantively applicable to e-commerce. Regarding procedural rules, particularly in connection with the probative value of electronic documents in civil and mercantile proceedings, there are no specific rules either in the Code of Civil Procedure or in the Mercantile Procedures Act.

1. Electronic transactions and electronic signatures

With regard to electronic transactions and electronic signatures, neither the Civil Code nor the Commercial Code explicitly regulates electronic contracting. However, by means of regulatory interpretation rather than a legal mandate, its rules applying to the formation and conclusion of contracts, as well as those determining the formalities to which contracts must conform, are applicable to electronic transactions.

a. Commerce and finance

For mercantile and financial matters, there are various explicit provisions recognizing the functional equivalence of printed documents with handwritten signatures and digital documents with digital signatures. Both the Banking Act and the Electronic Book-Entry Securities Law recognize the legal validity of electronic transactions and the use of electronic signature. Procedurally speaking, a number of articles in the Consumer Protection Act recognize the use of electronic media for certain acts.

Article 104 of the Consumer Protection Act authorizes notifications via any technical medium, whether electronic, magnetic or other, that provides written evidence and guarantees security and reliability. It also provides for authorities to use these media to issue summons, request information and conduct general procedural communications**.** Under article 121 of the law, requests for arbitration must include, among other things, the location or technical medium for notifications, while article 130 includes a requirement to designate the location or technical medium for receiving notifications as well where lawsuits must be filed.

The Banking Law governs financial intermediation and other operations by banks, with the oversight of the Central Reserve Bank of El Salvador and the Superintendency of the Financial System. Article 60 of this law provides that both credit and debit operations – in other words, interbank loans, systems for clearance of settlement operations, direct credits and debits, transfers related to State operations, transfers to and from foreign countries and other transactions between banks – may be conducted by electronic data exchange.

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 these systems. The certifications provided by the official authorized by the Central Bank to monitor and maintain records of said records and logs has enforcement powers against parties failing to meet their obligations. Instructions that banks send to the Central Bank are irrevocable. The law also obligates the banks to accept electronic instructions from other banks for debit or credit operations in the accounts of the (former) banks' clients.

Article 240 of the law obligates banks to provide accurate and timely information to the Central Bank that the latter requires to carry out its functions, and the banks must do so within the timeframe, in the form and via the media, that the Central Bank specifies.

The banks are also obligated to facilitate direct access to their computer systems for the Superintendency to obtain accounting, financial and credit information that it needs to fulfil its oversight function according to the law and the security confidentiality standards of the individual institutions and in accordance with their technical constraints. Failing to meet this obligation, providing information that is erroneous or that produces errors, and, on the part of Superintendency personnel, using information improperly, are acts punishable by a fine of up to 400 minimum times the monthly wages, except where other sanctions are specified in other laws, and without prejudice to any criminal liability that may be incurred.

As regards the securities market, the Electronic Book-Entry Securities Law also recognizes the use of electronic media for electronic transactions. Furthermore, under article 1 of this law, electronic book-entry securities represent negotiable transferable securities in an electronic record, and not in a hardcopy document. Generation, management and other acts affecting these registries, as well as their deletion, are subject to the provisions of this law, and, in cases where this is not applicable, to the Securities Market Act and the other mercantile laws, as appropriate to the nature of electronic registries of electronic book-entries and normal securities market practices and customs.

It also establishes that dematerialized 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. Stocks and non-group-issued securities can be represented by paper securities or electronic book-entries, as the issuer decides.

Among the principal concepts behind the principle of functional equivalency established in article 2 of the law are the following:

(i) Dematerialized or registered security: types of securities represented by a book-entry;

(ii) Electronic book-entry of securities: accounting notation made in an electronic record of securities accounts maintained by a depository institution. This constitutes proof of the existence of dematerialized securities, as well as of the obligations of its issuer and the rights of its legitimate owner;

(iii) Electronic Registry of Securities Accounts: compilation of accounting entries relating to the existence of registered securities and actions affecting them;

(iv) Electronic Registry of Issues Deposits: compilation of issues delivered to the depository for deposit and administration. It electronically documents actions that create, modify or extinguish an issue of dematerialized securities and actions that encumber or affect book-entries that make up each issue. The record of an issue authorizes the depository to form book-entries for each issue.

(v) Dematerialization or divestiture of securities: a process that results in the legal conversion of paper securities to electronic book-entry securities; and

(vi) Materialization or incorporation of securities: a process that legally converts book-entry securities to paper securities.

Article 4 allows issuers of stocks represented by book-entry securities to maintain an electronic registry of shareholders in place of the traditional shareholder registry book. It must contain the information on the characteristics of the stock, the names of stockholders, their domiciles and places of residence, the number and type of shares that they have and any encumbrances, along with related information.

Article 30 obligates depositories to keep an electronic record of issues deposits, documenting the issues deposited and any actions that modify them or that affect or annul the legal effects of the issues. Article 65 of the law authorizes depositories to use electronic or magnetic means of data transmission and storage, to request and send information to the entities participating in the securities market, and to keep their files, minutes and other documents.

Article 37 of the law establishes the Electronic Registry of Securities Accounts, which is an accounting record composed of the accounts of securities deposits that depositors have opened at the depositories, these being firms specializing in the deposit and custody of securities. For acts affecting the validity of the securities, such as encumbrances, the records or other legal acts affecting the registered securities, in order to be valid, must be registered in said record.

2. Consumer protection

In terms of consumer protection, the Salvadoran Constitution recognizes the protection of consumers' interests as a fundamental right, and prohibits monopolistic practices, which are considered harmful to consumers. Based on the Constitution, the Congress passed the Consumer Protection Act, which incorporates various precepts of United Nations General Assembly Resolution 39/248 dealing with consumer protection guidelines, among which are consumers' right to information, as well as the right to access safe products. The law does not establish specific provisions on e-commerce, but since it does not distinguish the media by which providers offer their products and consumers acquire them, the general rules apply to online transactions.

Thus, article 4 recognizes the following fundamental rights of consumers:

> (i) To receive from the provider information that is complete, accurate, truthful, clear and timely regarding the characteristics of the products and services to be acquired, as well as on their risks or side effects, if any, and on the conditions surrounding the contract;
>
> (ii) To be protected from misleading or false advertising;
>
> (iii) To acquire goods and services in the conditions and on the terms that the provider publicly offered;
>
> (iv) To be educated and informed on consumer issues;
>
> (v) To have free choice and equal treatment in similar circumstances without discrimination or abuse of any type;
>
> (vi) To be protected against the risk of receiving products or services that jeopardize life, health or personal integrity;
>
> (vii) To demand and receive compensation if the quality, quantity or form of products or services delivered differ from those offered, with the option of having the good repaired, demanding performance of the offer if possible, having the price of or fee/rate for the service reduced, accepting a different product or service, or being reimbursed the amount paid;
>
> (viii) To be protected from abusive practices and the inclusion of abusive clauses in contracts;
>
> (ix) To demand in court or by various means of alternative dispute resolution reparation for damages suffered because of the deficiency, poor quality or delayed delivery of goods and services acquired; and
>
> (x) To have access to a complete reading and explanation of all obligations and conditions stipulated in the contract and its attachments to which the parties are committing themselves.

3. Privacy and data protection

As regards the protection of personal information and the right to privacy, El Salvador has signed the American Convention on Human Rights, and has incorporated as a fundamental right in various provisions of its Constitution the right to personal and family privacy and the individual´s right to his/her personal image. It also establishes personal honour and privacy as constraints on freedom of expression. Article 24 also prohibits interference and intervention in telecommunications. However, it authorizes temporary intervention via written and well-founded judicial mandate in exceptional cases, although requiring that private matters not related to the matter motivating the exception to be kept in secret. Illegally obtained information is inadmissible.

It also recognizes that each person has the right to a name that identifies him or her, and that, as an attribute of all natural persons and as a means of individualization and identification, the name must be protected by the State through statutory regulations.

Thus, the Congress passed the Natural Persons Names Act, which contains a number of measures protecting the holder of a name against its improper use. Among these measures, the law provides criminal sanctions for people who change their names to create false identities. It also stipulates that when names are usurped, the person whose name has been usurped has the legal right to sue in order to stop the abuse. It also provides that a person who improperly uses the name of another and applies it to a fictitious person, adopts it as a pseudonym or in any other way, can be obligated to cease such improper or undue use, or to make the necessary changes.

As concerns financial matters, article 232 of the Banking Act provides that information on deposits and savings received by banks shall be confidential, and that information on such operations may be disclosed only to the account holders, their legal representatives and the Directorate of Internal Revenue when this is required for oversight purposes. Other operations are subject to confidentiality, and can be divulged only to authorized officials and those demonstrating both a legitimate interest and authorization from the Superintendency. An exception to this confidentiality provision occurs when information is requested by the Directorate of Internal Revenue for oversight purposes. The law also provides that banking confidentiality shall not be used to obstruct the investigation of crimes, determination of taxes or collection of tax obligations, or to prevent garnishment of assets.

Article 61 of the Banking Act provides that the Superintendency is to maintain a credit information service with information on the users of institutions in the financial system, in order to facilitate the institutions' assessment of the risks of their operations, which may be delegated to a private entity. The banks and other institutions overseen by the Superintendency are obliged to provide the information that the Superintendency requests.

As regards confidentiality in the securities market, under article 63 of the Electronic Book-Entry Securities Law, securities deposits received by depositories are subject to confidentiality, and information on these operations may be given only to account holders or their legitimate representatives. It also establishes that such confidentiality shall not be used to obstruct the investigation of crimes or prevent garnishment of assets, or to obstruct the Superintendency's oversight function, while the rest of the information contained in the Registries of Shareholders and of Book-Entry Securities remains subject to confidentiality and can only be given to the courts, the General Prosecutor of the Republic or other authorities in the exercise of their legal authority, provided that their action has first been authorized by the Superintendency.

In the customs area, the Customs Simplification Act establishes the obligation to maintain the confidentiality of the personal and normative information of those executing digital signatures that have been digitally certified and those filing or storing information on the certifying entities in databases that, for all legal purposes, are to be considered private, in order to ensure the confidentiality of information and respect for and protection of personal privacy. Exceptions are permitted if the General Prosecutor of the Republic or a court with appropriate jurisdiction demands such information for well-founded reasons.

Under the Act, such personal information can in no case be crossed-referenced, profiled or used for purposes other than those provided for in the Act, except if the person to whom the information pertains agrees expressly in writing to its use for a purpose different from that for which the information was collected, processed and recorded or stored.

The Act also obligates employees, officials and users of the Customs Service, as well as other persons authorized to use the computer systems and the media that are provided for the transmission of electronic data and communication with the Customs Service, to observe the security measures established by Customs, including those relating to the use of codes, confidential passwords and security codes.

4. Intellectual property

In relation to intellectual property, the Constitution authorizes the granting of privileges for a limited time to discoverers, inventors and improvers of productive processes. In this connection, as part of the copyright regime, the Intellectual Property Act protects artistic and literary works – including computer programs – and compilations, a category that includes computer databases. The law 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 via any medium.

The Trademarks and Other Distinguishing Marks Act recognizes that acts of unfair competition, which is to say those conducted 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 law permits the use of electronic media to register distinguishing marks. This provision is consistent with the law on uniform procedures for the presentation, processing and registering or deposit of instruments in the Registries of Real Estate and Mortgages, Commercially Owned Real Estate, Commerce and Intellectual Property, providing for the use of fax and e-mail addresses in requests for recording of instruments in these registries, for use by registry personnel to notify requesting parties.

As regards international commitments, El Salvador has ratified:

- The WIPO Copyright Treaty (WCT) and Performances and Phonograms Treaty (WPPT)
- The Universal Copyright Convention
- The Brussels Convention Relating to the Distribution of Programme-Carrying Signals Transmitted by Satellite
- The Central American Convention on the Protection of Industrial Property
- The United States-Central America-Dominican Republic Free Trade Agreement
- The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) administered by the World Trade Organization (WTO)

5. 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 law is consistent with CAFTA-DR, and its article 113-A provides that in cases of online cyberpiracy of trademarks, the national entity responsible for administering the country code top-level domain (Asociación SVNet) must have 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, observing the legal provisions relating to the protection of their privacy.

In this regard, the Asociación SVNET (NIC El Salvador), which is the entity responsible for issuing and updating policies for the functioning of the top-level domain ".sv" has put in place a Uniform Dispute-Resolution Policy and related regulations, establishing rules on arbitration to resolve domain name disputes. The policy recognizes the Center for Mediation and Arbitration of the American Chambers of Commerce (AMCHAMs), for arbitration purposes. However, the instruments adopted by the Asociación SVNET make no reference to the ICANN Uniform Domain-Name Dispute-Resolution Policy.

6. Cybercrime

On the criminal side, article 12 of the Law Against Acts of Terrorism defines cybercrimes and provides for prison sentences of 10 to 15 years 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/communication/telematics systems associated with public, social, administrative, emergency or natural 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 above-mentioned effects.

Article 24 of the Special Law to Sanction Customs Violations specifies 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 his/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 fraudulent); and (v) manipulating the computer or communications systems in order to obstruct any control function that the system provides for.

It should be noted that article 23 of this law provides for prison sentences of 3 to 6 years for those creating, hiding, falsifying or totally or partially altering information that is of importance to the customs taxation system, or destroying accounting records or tax control records, auxiliary records, financial statements and attachments, files, records, merchandise, documents, or computer systems and programs or magnetic media backing up or containing said information. Both persons directly participating in such creating, hiding, altering or expressly destroying, and those planning and giving the order for such action, are considered guilty of this crime.

Procedurally, article 45 of the Law against Acts of Terrorism admits as evidence a statement of an undercover agent, victim or witness made through electronic media with voice and image distortion, if the medium allows for real time questioning, and if, for good reason, said agent, victim or witness cannot appear in person before the relevant authorities.

Except for the articles previously mentioned in the Law against Acts of Terrorism and the Special Law to Sanction Customs Violations, neither the Penal Code nor the Criminal Procedures Code refer to cybercrimes or to data messages. However, the provisions of these laws can be applied to cybercrime. The assessment of information-technology elements involved in the crime are the responsibility of ministerial and judicial authorities.

7. Taxes and customs

The Tax Code authorizes tax declarations via electronic communications networks such as the Internet, magnetic media and other means of data transmission such as email, the security criteria for which are set forth in the Tax Code Regulations. It also authorizes the Tax Administration to send notifications via email and other traceable electronic communications media. It also authorizes the Tax Administration to use media of its own, available through technological advances, to access the billing systems of financial institutions and alike, as well as credit card management systems. The Code recognizes the full probative value of unalterable optical images, obtained by the Tax Administration, of original documents related to the taxes that it administers.

The Customs Simplification Act is an important advance for electronic transactions, since it incorporates measures consistent with RECAUCA and CAFTA-DR, and contains some provisions aligned with the UNCITRAL Model Law on Electronic Signatures. The act's principal object is to establish a basic legal framework for the adoption of mechanisms to simplify, facilitate and monitor customs operations by using automatic information exchange systems, under the supervision of the Customs Service.

The principal measures include authorizing passive and active users of the Customs Service to electronically transmit documents, including merchandise declarations, certifications or certificates of origin, bills of lading, shipping manifestos and any other documents needed for foreign trade operations. This also authorizes payment of customs obligations by electronic funds transfer from the bank accounts of those declaring items, payments of customs agents and of third parties, to the checking account of the Office of the Treasury.

The law further establishes rules for the functioning of remote customs clearance systems for transmitting customs declarations for goods, to be effected by electronic transmission of tax-related information between the Customs Service, users, entities that assist the customs service, as well as banks, traders and institutions that oversee foreign trade.

It also stipulates that documents contained in magnetic, digital or electronic media have the same legal value as those on paper, and mandates that information in paper form, as well as electronic messages, be preserved or archived in their original form in order to make them accessible for later consultation. In this connection, it also establishes that no provision prohibiting the admission of data messages as evidence shall be imposed in any legal proceeding. The law 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 attached documents, and

as a way of certifying payment of amounts due, and that their use is to have the same legal effects 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 law establishes systems to certify the information transmitted. Such systems are to be operated by certification entities authorized by the Ministry of Finance, which has oversight and sanctioning power over them. The law states that certifying entities must be juridical persons with the technological training to generate and certify digital signatures, and that they must have the power to publicly vouch for the electronic transmission of data on the dates and hours when it occurred, in order to guarantee that communications cannot be contested.

The law establishes that for the execution of the different acts that make up the remote customs clearance system and for the exchange of general information, each authorized user will have a pair of interconnected passwords or unique keys, one public and the other private, so that each corresponds exclusively to the other, and with the certifying entity administering a system for the issuing of public keys. The association between the two types of keys constitutes the digital or electronic signature, which for all legal purposes is the digital equivalent of the written signature, and permits a recipient of an electronic message to be certain of the sender's identity, preventing the latter from later denying authorship of the message.

Users of the system, as well as subscribers, are obligated to maintain the confidentiality of the private keys assigned to them, and are liable for the legal consequences of their improper use, regardless of whether such use is by them or by unauthorized third parties.

8. Legislative initiatives

The principal legislative initiatives being reviewed by the Congress include a Data Protection bill, as well as an Electronic Communication and Signature bill, the object of which is to regulate electronic signature in general and apply it to other areas, without its being limited to foreign trade. It also includes provisions to protect consumers in their relations with providers of certification services.

(D) Guatemala

The Electronic Communications and Signature Recognition Act is the main provision governing e-commerce. However, various civil, mercantile, financial, administrative and penal laws are also applicable in specific ways, as described below.

1. Electronic transactions and electronic signatures

Of note with respect to electronic transactions on the international level are CAFTA-DR and RECAUCA, while there is a national provision, Decree 47-2008, which mandated the promulgation of the Electronic Communications and Signatures Recognition Act. This applies to all types of electronic communication, transactions and other legal acts, whether public or private, national or international, with the exceptions set forth in the law.

a. Commerce and finance

Article 2 of the Electronic Communications and Signatures Recognition Act establishes that e-commerce is to include the elements of all sorts of commercial relationships, contractual and other, structured on the basis of the use of one or more electronic communications or communications of any similar type.

Commercial relationships include, though they are not limited to: any commercial operation to supply or exchange goods or services; any distribution agreement; any operation involving trade representation or involved in documentations for trade transactions; any type of financial operation, including factoring and leasing of equipment with option to purchase; construction of public works; consulting; engineering; granting of licenses; investment; financing; banking; insurance; concessions or agreements to provide a public service on a commercial basis; joint ventures and other forms of industrial or commercial cooperation; and transportation of merchandise or passengers by air, sea, rail or road.

The law, which incorporates various principles of the UNCITRAL Model Laws on Electronic Commerce and the Model Law on Electronic Signatures, applies to all types of electronic communication, transactions or legal acts, whether public or private, domestic or international, with the exceptions specified in the law pursuant to international treaties or legal mandate. It specifies legal requirements that electronic communications must meet, as well as the elements that must be present for the formation and development of contracts through electronic media.

The law also defines the characteristics that electronic signatures and digital certificates are required to have, and the functions of certification service providers. It authorizes the Ministry of Economy to create and organize a Registry of Certification Service Providers, and to inspect, monitor and oversee certification service providers.

The law furthermore recognizes the functional equivalence of signed printed documents and electronic documents with advanced electronic signature backed by a digital certificate. It includes provisions governing specific topics such as the transport of merchandise and measures to protect consumers in online transactions.

The Civil Code establishes principles governing the 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. In addition, Decree 42-2006 reformed the Civil Code by adding section 8 of article 1131, which regulates various aspects of physical signatures and the seal of the chief registrar, alternate registrar or assistant registrar authorizing the registry operation and executing the registry seal.

Under this section, physical signatures may be replaced by signatures that are electronic, digitized or printed via any electronic medium, and these have the same legal force as physical signatures, provided that the security standards established and approved by the Registry to guarantee their legitimacy are fulfilled.

The Commercial Code, which regulates merchants' mercantile activities, requires that documentation and information related to such activities be preserved for five years, and that certain types of acts be recorded in the Mercantile Registry or in the associated books or systems.

In the financial area, article 4 of the Organic Law of the Bank of Guatemala authorizes this institution to take measures to ensure the proper functioning of the settlements systems, pursuant to the guidelines issued by the Monetary Board. Accordingly, the Monetary Board issued Regulations on the Real Time Gross Settlement System (Sistema de Liquidación Bruta en Tiempo Real, or LBTR), which, among other things, covers the use of digital signatures by public- and private-sector financial institutions. In addition, article 63 of Decree 34-96, by virtue of which the Securities and Merchandise Market Act was promulgated, authorizes oversight and accounting for operations involving securities represented by accounting entries, to be carried out by normal accounting, documentary or electronic procedures.

(b) Government

As regards electronic transactions with the government, relevant instruments include Decree 27-2009, the Congressional Reforms to Decree 57-92 and the State Contracting Act, which establishes the operational basis for the online government procurement system (GUATEMCOPRAS), which can be used by State entities, decentralized and autonomous entities, executing units, municipal governments and State or municipal public enterprises, under the article 1 of the act.

Under article 23, entities involved in the quotation and bidding processes must publish in GUATECOMPRAS the basis for quotes or bids, the relevant technical specifications, evaluation criteria, questions and answers, lists of bidders, documents certifying the awarding of bids, and information on hiring and procurement contracts. Article 35 authorizes electronic notification via GUATECOMPRAS, and article 39bis allows changes to the quotationbasis to be published on the system.

In addition to the Regulations to the State Contracting Act (which sets forth the authority of the State Contracts and Procurements Regulations Direction), the Ministerial Agreement 1-2006 (on the Management Linkage System, or SIGES), the Integrated Accounting System (SICOIN) and the

GUATECOMPRAS system, there is the State Contracting Regulations Direction Resolution 30-2009, which legally recognizes the Internet URL of the State Contracting and Procurement Information System (www.guatecompras.gt), specifying, among other things, the types of users who may use the system and the criteria under which the Regulations Direction is to manage access to the system's accounts.

2. Consumer protection

In the area of consumer protection, article 119 of the Guatemalan Constitution establishes a State mandate to prevent excessive practices that lead to a concentration of goods and means of production 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 consistent with health, safety and legitimate economic interests. In addition, article 130 protects consumers by prohibiting monopolies and special privileges.

On the basis of the Constitutional mandate to protect consumers' interests, Congressional Decree 6-2003, approving the Consumer and User Protection Act, was issued. Also, the Law to Promote Competition and Effective Consumer Protection incorporates the basic principles of consumer relations set forth in United Nations General Assembly Resolution 39/248, which deals with Consumer Protection Guidelines. The law states that the rights and guarantees it provides for are inalienable and are in the public interest.

Article 4 enshrines various consumers' and users' rights, including:

(i) protection against risks that can jeopardize life and safety as a result of the acquisition, consumption and use of goods and services;

(ii) freedom to chose goods and services;

(iii) freedom for contracting;

(iv) information that is true, sufficient, clear and timely regarding the different goods and services, indicating whether these are new, used or refurbished, as well as their potential risks;

(v) repair, indemnification, reimbursement or exchange of goods when the agreed commitments in a transaction, and the legal provisions establishing the provider's liability for hidden deficiencies, have not been met;

(vi) replacement of product, or in the absence of this, the option of a credit for its value, to be used in purchasing another product, plus the option of reimbursement for the excess price paid if a product is inferior in quality or quantity from that promised; and

(vii) education on the proper consumption and use of goods and services, and on how related rights and obligations may be exercised, to mention the most important educational elements.

In addition, article 51 establishes a consumer's right to withdraw from an agreement within five business days of signing a contract or of the date on which a contract is signed outside of a commercial establishment – specifically, by telephone or at the consumer's or user's place of residence.

The law obligates providers to respect the terms of their offers, promotions, advertising and membership contracts. In the case of standard-format contracts, it also requires legibility and the use of Spanish language. The law does not specify the medium in which contracts must be presented. In other words, it does not call for any special treatment for online operations in contrast to traditional operations.

3. Privacy and data protection

As regards the protection of personal information, article 24 of the Guatemalan Constitution protects privacy by enshrining as a fundamental right the inviolability of private correspondence and telephonic, radio, cable and other communications that use modern technology. Information obtained in violation of this article is considered unreliable and is not admissible as evidence in judicial proceedings.

Article 30 establishes as a principle the public nature of all administrative acts, excepting those related to military or diplomatic affairs that have national security implications, or data provided by private parties under the guarantee of confidentiality.

Article 31 states that all persons have the right to know about the information concerning them that is in form of files, papers, archives or any other type of governmental record, and to know the purposes for which such information is being used, as well as the right to correct, rectify and update such information.

To this end, the Tax Code protects the confidentiality of tax information. Under Article 101A of the Code, revealing the amount of tax paid, or amounts of profits, losses, costs or any other data in the revised accounts of individual or juridical persons is punishable. The Code also specifies that documents or information obtained in violation of this article are considered unreliable and are not admissible as evidence in judicial proceedings.

Article 30A of the Code authorizes the Superintendency of Tax Administration to require any natural or juridical person to periodically or at specified times to provide information on mercantile relations, acts or contracts with third parties or entities that are the source of taxes, in written, electronic or other appropriate media, provided that said relations, acts, contracts or entities are related to tax matters and do not violate professional confidentiality or the Constitutional guarantee of confidentiality. Any information provided to the Superintendency of Tax Administration is provided under conditions of confidentiality.

In the financial area, article 63 of Decree 19-2002, The Banks and Financial Groups Act, regulates banking confidentiality and provides that, except for obligations and duties under legal provisions relating to the laundering of money and other assets, bank managers, legal representatives, officials and employees may not provide information in any form to any natural or juridical, public or private person, that may violate the confidential character of the identity of depositors in banks, financial institutions or firms within a financial group, or information provided to these entities by private parties. This constraint does not apply to information that banks are required to provide to financial authorities, who are similarly prohibited from revealing it except under judicial order.

Article 217 of the Penal Code specifies violating the confidentiality of private correspondence and papers as a crime, and provides for imposing fines on persons who deliberately, or in order to obtain secrets concerning another person, open correspondence or view sealed bids, telegrams, telephone calls or other communications not addressed to them, or who, without opening them, access their content. Article 219 provides punishment for the crime of intercepting communications, by sanctioning the use of fraudulent means to intercept, copy or record televised, radio, telegraphic, telephonic communications or the like, or obstructing or interrupting them.

Article 1 of Congressional Decree 57-2008 approved the Public Information Access Act, whose objectives include guaranteeing individuals the right to knowledge and protection of personal information concerning them that is held in State files, as well as the right to update such information.

Article 9 defines personal information as any information concerning identified or identifiable natural persons. It also establishes that so-called sensitive data and sensitive personal data are such because they refer to the physical or moral characteristics of persons, or to facts or circumstances of their private lives or activities, such as personal habits, racial or ethnic origin, ideology and political opinions, religious beliefs or convictions, state of physical or mental health, sexual preference and sex life, moral and family situation and other such private matters.

Article 9 also establishes the right of habeas data, guaranteeing all persons the exercise of their right to know the information concerning themselves that is held in public files, papers, archives, records or any

other medium, and to know the purposes for which such information is being used, as well as the right to its protection, correction, rectification and updating. Non-personal data not associated with identifiable persons, such as demographic information gathered for statistical purposes, is not subject to habeas data or to this law's personal information protection provisions. Article 30 establishes various obligations incumbent on compelled subjects[3] – parties subject to these obligations – regarding the treatment of personal information, as part of giving full effect to habeas data.

Article 31 establishes that compelled subjects may not disseminate, distribute or market the personal data contained in information systems involved in the exercise of their functions, except with the express written consent of the individual/s to whom the information refer/s. Marketing sensitive data or sensitive personal data is also prohibited by any medium. Under article 34, the persons to whom personal information pertains, or their legal representatives, may, once their status is accredited, modify personal data pertaining to them in any information system.

Under article 36, public information that is or can be localized in administrative files may not be destroyed, altered, modified, mutilated or hidden by the public servants producing, processing, administering, filing or safeguarding them, unless such action is part of their public duties and is legally justified. In addition, article 55 governs when appeals to review proceed, while article 67 provides for sanctioning public servants, officials or employees who disclose or facilitate the disclosure of information that they have knowledge of by virtue of their job, and which, by law or under the Constitution, is confidential or proprietary. The sanction provided for is a prison sentence of five to eight years, plus a ban from public service for twice the period of the sentence imposed, in addition to a fine of 50,000 to 100,000 quetzales. These criminal sanctions apply without prejudice to any civil liabilities and damages that may be incurred by revealing confidential or proprietary information.

4. Intellectual property

Article 42 of the Constitution recognizes copyright and inventors' rights, giving their holders exclusive ownership of their works and inventions, in conformity with international law and treaties. In this connection, article 59 of the Constitution makes it a primary obligation of the State to protect, encourage and disseminate the national culture, as well to promote and regulate scientific research and the creation and use of appropriate technology.

The Copyright and Related Rights Act protects the copyrights of creators of artistic, scientific and literary works. The works subject to protection include both computer programs and databases. The law also defines any permanent or temporary storage of a work in any material form, format or medium as a reproduction.

As regards the related rights of artists, performers, producers of phonograms and broadcasting organization, the law defines the concepts of phonograms and videograms and recognizes the right of public communication by any analog or digital medium or procedure.

The terms of article 274 of Guatemala's Penal Code provides for prison sentences of four to six years, plus a fine, for: (i) false attribution of copyright holder, artist, performer, producer of a phonogram or

[3] Under article 6 of the Public Information Access Act, a compelled subject (*sujeto obligado*) is any public or private natural or juridical person of any type, national or international, and any State institution, organization, organ, entity, office, or other that manages, administers or executes public resources, State assets or documents of public administration in general, that is obligated to provide the public information requested of it, including, among others, the Executive Branch and all of its agencies, centralized and decentralized as well as autonomous, the legislature and all of the entities that are a part of if, the Judicial Branch and all the entities that are a part of it, all centralized, decentralized and autonomous entities, and the Constitutional Court.

broadcasting organization, whether or not for the purpose of economic exploitation; (ii) presentation, performance or public playing, transmission, communication, broadcast and/or distribution of a protected literary or artistic work without the authorization of the copyright holder, except in cases provided for by law; (iii) public performance or transmission of a protected phonogram without the authorization of its producer, except in cases provided for by law; and (iv) reproduction or rental of copies of protected literary, artistic or scientific works, among others, without the authorization of the copyright holder.

The Industrial Property Act does not regard economic, advertising or business methods, or, in isolation, computer programs, as being subject to patent protection. Article 275 specifies as crimes: (i) revealing to a third party an industrial secret to which one is privy by virtue of work, job, position, professional practice or business relationship, or by virtue of a license for use of the information, without the consent of the holder of the industrial secret, having been advised of the confidentiality of the information, in order to obtain an economic benefit for him/herself or for a third party, or to cause damage to said holder or to the authorized user of the information; (ii) using the information contained in an industrial secret that is known by virtue of a person's work, job, position, professional practice or business relationship without the consent of the person holding the industrial secret or of its authorized user, or that has been divulged by a third party, provided that such party did not have the consent of the person holding the industrial secret or of its authorized user, in order to obtain an economic benefit for his/herself or for a third party, or to cause damage to said holder of the industrial secret or of its authorized user.

Article 275bis of the Penal Code provides for prison sentences of four to six years, plus a fine, for commercial use of a registered trademark or unauthorized copy or fraudulent imitation thereof, involving products or services identical or similar to those to which the trademark applies.

On the international intellectual and industrial property rights front, Guatemala has ratified:

- The WIPO Copyright Treaty (WCT) and Performances and Phonograms Treaty (WPPT)
- The United States-Central America-Dominican Republic Free Trade Agreement
- The Lisbon Agreement for the Protection of Designations of Origin and their International Registration
- The Paris Convention for the Protection of Industrial Property (1883)
- The Berne Convention for the Protection of Literary and Artistic Works
- The Geneva Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of their Phonograms
- The Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations
- The WIPO Patent Cooperation Treaty (PCT)
- The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), administered by the World Trade Organization (WTO).

5. Domain names

The Domain Name Dispute Resolution Centre for the top-level domain name ".gt" (Guatemala), housed at Guatemala'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 the Internet Corporation for Assigned Names and Numbers (ICANN).

6. Cybercrime

In the area of cybercrime, Guatemala's Penal code provides for various sanctions for the crimes specified in articles 274A to 274G, including prison sentences and fines for: (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 a natural or juridical person; and (vi) distributing destructive computer programs.

Article 295 provides sanctions for attacking the security of telecommunications or postal communications, or interrupting or obstructing such services by any means.

7. Taxes and customs

In the tax area, article 98A of the Tax Code authorizes the Tax Administration to: (i) by mutual agreement with the taxpayer, establish an e-mail address or electronic message service for each taxpayer or responsible party, for the purpose of acknowledging receipt of tax statements and payments made, and for sending information bulletins, summons, notifications and other communications relevant to the taxpayer, when appropriate; (ii) establish procedures for the creation, transmission and preservation of invoices, books, accounting records and documents by electronic means, copies of which may be used as evidence in judicial proceedings, whether printed or in another medium; and (iii) require taxpayers to pay taxes electronically, taking account of their economic capacity, volume of sales and access to computer networks.

In order for notifications made by electronic media to have probative value, article 133 requires that the notice or proof of receipt or delivery demonstrating that the notification was received or delivered to the taxpayer's e-mail address be printed on paper by the Tax Administration employee responsible for the notification, and that this be included in the relevant file.

In relation to taxpayers, the Tax Code authorizes meeting tax obligations through the use of electronic forms, as provided for in article 104. Article 105 permits passive users to submit their statements, including sworn statements, financial statements and attachments, or any information that the law requires them to provide, electronically, provided that the electronic media employed meet the following criteria: (i) identification is by means of a confidential electronic password that is equivalent to a signature; (ii) the integrity of the information submitted is ensured; (iii) the Tax Administration provides the passive user proof of receipt of the statement, attachment or information in a physical or electronic form.

The duly certified hard copy that the Tax Administration produced of statements, attachments and information submitted on paper, electronically or in other media is deemed authentic and of full probative value, in the absence of evidence suggesting that it should not be so considered.

Under article 125 of the Tax Code, acts of the Tax Administration consisting of issuing documents via computer, electronic, mechanical and other such means are legitimate, provided that these documents, which need not bear original signatures, contain the data, legal basis and information necessary for an accurate understanding of their origin and content. Similarly, authorizations made by the Tax Administration via electronic identification passwords are valid.

It should be noted that, consistent with the Tax Code, the Value Added Tax Act and the Income Tax Act, along with their corresponding regulations, also permit the use of electronic media for interaction between taxpayers and tax authorities, and for the purpose of meeting various tax obligations.

Finally, with regard to customs, Guatemala considers CAUCA and its regulations, as well as CAFTA-DR, applicable to its foreign trade operations.

8. Legislative initiatives

Among the legislative initiatives that have brought pending issues into the legislative process is bill 3715, which, among other things, deals with the harmonization of foreign digital signature certificates, as well as with the coordination of extrajudicial dispute resolution systems to solve disputes related to e-commerce operations.

(E) Honduras

Honduran legislation includes no special law regulating e-commerce or electronic contracting, but various general civil and mercantile legal provisions are applicable in these areas. In addition, Civil Code provisions on the formation and development of contracts, as well as the legal provisions that determine the

formal procedure requirements that they must meet, are applicable to electronic transactions. However, such application is the result of regulatory interpretation of the law, rather than explicit language.

1. Electronic transactions and electronic signatures

a. Commerce and finance

The Honduran Commercial Code has the particular characteristic that, though a single normative text, it governs various types of issues. Thus, unlike the other countries, which have opted to separate different matters and regulate them with specific laws, Honduras covers commercial and mercantile issues, trademarks, patents, banking operations, insurance contracts, maritime transport, bankruptcy and suspension of payments, among other things, in a single law. However, the Commercial Code does not explicitly regulate e-commerce or electronic contracting, and only has isolated provisions that may be applicable in these areas.

Under article 382, merchants who publish information on their characteristics as merchants, via broadcast media and other similar media, are obligated, under the terms of such advertising, to any third parties who in good faith have followed normal mercantile procedure. Under article 717, offers and acceptances made by telephone, cell phone or similar media are deemed to have been made between parties that are present, when the parties, their representatives or others working under their direct orders have communicated personally.

Article 441 permits merchants to conduct their accounting via electronic systems, while article 448 requires all merchants to keep for five years, in orderly fashion: accounting records and special books and records; documents; bills; ingoing and outgoing correspondence; background information related to tax obligations; and, where relevant, programs, sub-programs and other records processed through electronic or computer systems.

On the international front, the Honduran government has signed the United Nations Convention on the Use of Electronic Communications in International Contracts (CUECIC).[4]

Article 50 of the Financial System Act permits institutions in the system to offer and provide financial products and services via electronic media, for which purpose the National Banks and Insurance Commission is mandated to issue general rules regulating such operations. Accordingly, the Commission issued Circular CNBS No. 119/2005, Resolution No. 1301/22-11-2005, Standards Governing the Administration of Information and Communication Technologies in Institutions of the Financial System.

Article 51 of the Financial System Act recognizes the legal force of electronic signature, which accords data in electronic form the same legal value as written signatures on paper documents, provided that the 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.

With regard to the securities market, article 23 of the Securities Market Act authorizes securities exchanges to use electronic media and procedures in executing investors' orders and instructions. Article 60 obligates securities exchange member firms to verify the authenticity of securities handled by a Centralized Securities Deposit, whether these securities are stored in physical or intangible form.

Article 65 of the Act authorizes securities exchange member firms to provide their clients with a data processing and information system. In regard to securities intermediation contracts, article 72 specifies that

[4] The legislature has approved the Convention, which is to be submitted for ratification.

parties to such contracts may execute specific account operations or movements by e-mail, and may use e-mail for sending, exchanging and confirming investors' orders.

Under section 5 of article 72, if the parties agree to use electronic, computerized or telecommunications media to transmit orders, the orders must include reciprocal identification keys and set forth the responsibilities that accompany their use. The agreed identification keys will replace the parties' physical signatures, and thus documents or technical media in which the keys appear have the same force as documents signed by the parties, and the same probative value.

(b) Government

In the administrative realm, article 5 of the State Contracting Act provides for the use of information technologies in managing contracting systems to automate and publicize procedures. The Registries of Providers and Contractors are to be maintained in electronic form so as to increase the efficiency of public administration.

The Property Act, which, pursuant to its article 2, applies to personal, real, mercantile and intellectual property, as well as real and other rights, establishes measures designed to make legal proceedings in these areas expeditious, effective, transparent and fair. In this connection, article 28 establishes a Uniform Property Registry for which the Property Institute is responsible. This registry is composed of: (i) the Real Property Registry; (ii) the Personal Property Registry (which includes vehicles); (iii) the Mercantile Registry; (iv) the Intellectual Property Registry; (v) the Special Registries (including awards, concessions and geographical information, etc.); and (vi) Associated Registries (such as the Aircraft Registry).

Among the law's objectives, article 3 specifies the use of advanced legal, administrative and technological instruments to ensure the security, transparency, cost-effectiveness and time-reduction of recordable transactions and administrative procedures. Article 5 gives the Property Institute various authorities, including the administration and supervision of uniform procedures to ensure the rapid, economical and secure creation, recognition, transmission, transfer, modification, encumbrance and settlement of property rights subject to registry.

Article 53 permits the use of electronic media to pay the fees required to register documents or contracts in the various registries. As regards notarial protocol, article 112 permits notaries to conduct their procedures in electronic form, under security and confidentiality parameters established by the Property Institute. In addition, article 113 requires all acts, contracts and documents authorized or certified by a notary in electronic form to be incorporated in a database created for the purpose by the Property Institute. Original signatures and documents must be incorporated in the digital protocol as attachments.

Article 116 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, fingerprints to identify those appearing, and other means permitted by technological developments.

Under article 117, official instruments or contracts that must be registered and authorized by a notary can be transmitted for registration electronically. The electronically transmitted information is to be registered as a preliminary notation pending the submission and recording of specific original physical documents.

Article 120 provides for fees, taxes or duties deriving from the notarial authorization or certification of legal instruments, contracts or documents to be settled electronically by crediting an account or by some other electronic means of payment specified by the Property Institute.

Under article 124, fines of 20 to 50 times the amount of monthly wages can be imposed, without prejudice to civil and penal liability, for: (i) altering the content of the certified items, entries and records; (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.

Article 129 authorizes the Property Institute to create a mechanism for the issuance of 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.

2. Consumer protection

Article 331 of the Honduran Constitution obligates the State to recognize, guarantee and promote consumer freedom, and article 339 prohibits monopolies, monopsonies, oligopolies, hoarding and similar practices in industrial and mercantile activities.

In addition, the Consumer Protection Act incorporates in Honduran law the fundamental consumer rights provided for in United Nations General Assembly Resolution 39/248, which deals with the Consumer Protection Guidelines, including consumers' right to information and the right to have access to safe products.

Except for article 58 – which defines "sale by mail and the like" as offers of goods and services made via postal mail, telecommunications, electronic media and similar media, and accepted by these same media – the law has no provisions directly referencing e-commerce. However, online transactions are subject to the rules regarding consumers' right to clear information in Spanish, with legible characters, that is truthful, complete and timely (including price information, and information on the quality of and guarantees applying to goods and services), as well as being subject to the prohibition on misleading advertising and abusive clauses in membership contracts. Article 84 permits the use of electronic media for notifications in alternative dispute resolution procedures.

Article 31 of the Credit Card Act renders null and void any clauses of contracts between credit card issuing firms and cardholders that allow the former to change contractual conditions by adding fees not agreed to by cardholders, unless accompanied by additional benefits that can be accepted or refused in writing or via other media, such as e-mail.

3. Privacy and data protection

With regard to the protection of personal information, article 76 of the Constitution of the Honduran Republic enshrines the right to honour, personal and family privacy and personal image, while article 182 provides for habeas data, which can be invoked only be persons whose personal or family information appears in public or private files or records.

Habeas data makes it possible to obtain access to information, prevent its transmission or disclosure, correct imprecise or erroneous data, update information, enforce confidentiality and remove false information from any private or public file or record in conventional, electronic and information technology media, if the information is detrimental to a person's honour, personal or family privacy or personal image. This guarantee does not apply to the confidentiality of journalistic sources, on which the Constitutional Panel of the Supreme Court is exclusively authorized to rule.

Article 100 of the Constitution recognizes the right of all persons to the inviolability and privacy of their communications, except in the case of judicial order to the contrary. Violated or stolen communications are not admissible in judicial proceedings.

In this connection, article 214 of the Penal Code provides sanctions for the unauthorized interception of communications or for causing them to be intercepted, whether the media that they employ are telephonic, fax, telegraphic, electronic, computerized, or of any other type. Sentences range from six to eight years in prison if the crime is committed by a private individual, and eight to twelve years if the perpetrator is a public official or employee. Article 215 of the Code also provides for prison sentences of three to six years for unjustifiably disclosing, or using for one's own or another's benefit, a secret to which one is privy by virtue of his/her job, work, profession or trade and thereby causing harm to someone.

Article 2 of the Public Information Transparency and Access Act sets forth this law's principal objectives, which include establishing mechanisms to ensure the protection, classification and security of public information and respect for restricted access to: (i) information classified as confidential by public entities; (ii) information provided to the State by private parties on a confidential basis; (iii) confidential personal information; and (iv) information that the law classifies as secret.

Article 3 sets forth the law's principal definitions, including the definition of confidential personal information. This concept covers information on ethnic or racial origin; physical, moral and emotional

characteristics; private residence, telephone number and e-mail address; participation in or affiliation with political organizations; political ideology; religious and philosophical beliefs; states of physical or mental health; personal or family assets; and any other information relating to a person's honour, personal or family privacy or own image.

Article 23 recognizes habeas data, and article 25 prohibits compelling any person to provide personal data that could cause discrimination or jeopardize the person in material or moral terms. Article 24 requires that personal information always be protected, and provides that an interested party, or the National Human Rights Commission on its own behalf or representing an affected party, or the Public Ministry, can sue for such protection. Access to personal information may only be provided under judicial decree or at the request of the person whose personal information is involved, or of that person's representatives or heirs.

Article 17 establishes criteria for classifying information as confidential, and provides that, without prejudice to the provisions of the law on the secrecy of data and processes, or to the confidentiality of personal information and information provided to the State by private parties under conditions of confidentiality, public information shall be classified as confidential when the harm that it could cause is greater than the public benefit of knowledge of it, or when disclosure of the information jeopardizes:

(i) the security of the State;
(ii) the life, safety or health of any person; humanitarian aid; legally protected interests of children and other persons; or the right of habeas data;
(iii) confidential investigations involving the prevention, investigation or prosecution of crime, or the carrying out of justice;
(iv) interests protected by the Constitution and by statutory law;
(v) the conducting of negotiations and international relations;
(vi) the country's economic, financial or monetary stability, or its governance.

Article 27 defines administrative violations consisting of illegally copying, capturing, viewing, disclosing or marketing confidential information, or refusing to give personal information to its legitimate owner, his or her heirs or an authorized authority. It also provides sanctions for cases, not specifically covered in the law, of gathering, capturing, transmitting or disclosing personal information, or refusing to correct or update it or to delete false information or confidential personal data contained in any file, record or database of an institution subject to this law. Sanctions are imposed without prejudice to the civil and/or criminal liability that may result.

4. Intellectual property

In the area of intellectual property, article 108 of the Honduran Constitution provides that all authors, inventors, producers and merchants have exclusive ownership of their works, inventions, trademarks and business names, pursuant to the law. It should be noted that these temporary benefits are not considered monopolies under article 339 of the Constitution.

The Copyright and Related Rights Act 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 under article 2. Article 39 cites databases, including as a right of ownership the authority to access or grant public access to computer databases via telecommunications media.

The law also deems any storage of a work in electronic form, whether permanent or temporary, a reproduction. With regard to the related rights of artists, performers and broadcasting organizations, it defines the concept of phonograms, and recognizes the right of publication in any medium.

Article 248 of the Penal Code sanctions theft of the copyright of literary, scientific or artistic works and others protected by the Copyright and Related Rights Act with prison sentences of three to six years, plus a fine of 50,000 to 100,000 lempiras. Article 248A applies the same sanctions to natural or juridical persons who, without authorization from the owners of the copyright or related rights, commercially exploit television signals transmitted by satellite, or reproduce or project videos, films or similar works, as well as to end users of the exploited works.

Under article 5 of the Industrial Property Act, computer programs considered in isolation are not inventions, and therefore are not patentable. Article 170 prohibits access to and disclosing of industrial secrets without the authorization of their legitimate owners, as unfair competition.

In addition, article 97 deems a distinguishing mark to be in use in business when:

(i) it is used in advertising, publications, commercial documents or written or oral communications, regardless of the medium of communication used; or
(ii) it is adopted as a domain name, e-mail address, name or designation in electronic or similar media that serve as vehicles for electronic communications or e-commerce.

Under article 139, the owners or legitimate possessors of well-known distinguishing marks have the authority to request the courts to order a cancellation or modification of the recording of a domain name or e-mail address that uses said mark in an unauthorized manner.

Article 249 of the Penal Code establishes prison sentences of three to six years, plus a fine of 50,000 to 100,000 lempiras, for the manufacture or offering for sale of articles that, given their name, brand, packaging, presentation or appearance, could be confused with similar products that are patented or registered to another person.

Article 251 establishes the same sentence for the falsification, imitation or fraudulent use of legal figures or assets protected by the Industrial Property Act.

On the international front, Honduras has ratified:

- The Paris Convention for the Protection of Industrial Property;
- The Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations;
- The Convention for the Protection of Producers of Phonograms;
- The Berne Convention for the Protection of Literary and Artistic Works;
- The Patent Cooperation Treaty (PCT);
- The WIPO Copyright Treaty (WCT) and Performances and Phonograms Treaty (WPPT);
- The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) administered by the World Trade Organization (WTO);
- The Central American Convention on the Protection of Industrial Property and CAFTA-RD.

5. Domain names

The Sustainable Development Network of Honduras (NIC Honduras - www.nic.hn) is responsible for administering the top-level domain name ".hn", and has incorporated the principles of the Uniform Domain-Name Dispute-Resolution Policy of the Internet Corporation for Assigned Names and Numbers (ICANN) in its dispute resolution policy and regulations.

6. Cybercrime

The Penal code includes a number of provisions for sanctioning crimes committed against computer systems or that use computer systems for their commission. Thus, article 254 of the Code establishes a prison sentence of three to five years 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. Article 255 also provides for prison sentences of three to six years for damaging media or channels of communication. Under article 271, the sentence increases to between three and six years if damage is done to a postal, telegraph, telephone, electrical, radio or other telecommunications medium.

Article 394E of the Code sanctions the destruction, hiding, or falsification 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 a natural or juridical person, in order to obtain, maintain or extend a capital or credit facility of a supervised institution, with prison sentences of three to six years when the amount of the benefit obtained does not exceed 10,000 lempiras, and with sentences of six to twelve years when the amount is above said level.

Article 394F of the Code provides prison sentences of six to twelve years for the destruction, hiding, or falsification of accounting records, company books, legal documents, certifications, affidavits, general records, financial statements, documents stored in magnetic or electronic form, or other information of a supervised institution in order to cover up, distort or maliciously modify credit or debit operations, direct or contingent obligations, illiquidity, insolvency or other facts that must be recorded in accounting records or other records.

Article 394-I sanctions 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 sentences specified are three to six years of prison when the fraud does not exceed 10,000 lempiras, and six to twelve years if it is above that amount. 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.

The Money Laundering Crimes Act deserves special mention. The primary object of this law is to prevent and punish the crime of assets laundering as a form of organized crime, as well as provide for precautionary measures to ensure the availability of the assets or instruments of such crimes.

Under article 43, the law gives the National Banks and Insurance Commission supervisory authority over those who, among other things: (i) conduct savings and loan operations; (ii) conduct systematic or substantial operations through magnetic, electronic, telephonic or other forms of communication; or issue, sell or purchase travelers' checks, postal money orders or any other monetary instrument or document**;** or (iii) conduct systematic or substantial transfers of funds.

7. Taxes and customs

As regards taxation, the Tax Code contains various important measures to facilitate online transactions. Article 47 is particularly important, since it permits taxpayers to issue proof of their activities through magnetic or electronic media. Article 43 establishes taxpayers' obligation to facilitate tax authorities' job of reviewing, verifying, monitoring, inspecting and investigating, as well as determining and collecting taxes, for which purpose they must maintain in orderly fashion and make available to the relevant authorities in their tax domicile, for a period of five years, accounting books, special books and records, documents and evidence of events that generate tax obligations, or, where relevant, programs, subprograms and other records processed by electronic or informatic means.

Article 49 permits financial institutions to provide tax authorities information on operations carried out with account holders, cardholders, savings account holders, users, depositors or clients that involve magnetic or electronic money transfers, with the periodicity required by said authorities, provided that the persons involved have given prior authorization for release of the information.

As regards customs, the General Customs Act does not mention the use of electronic media for customs clearance and related procedures, but does recognize the applicability of international treaties. Thus, CAUCA and RECAUCA, which do consider electronic media, are applicable. It is also important to note the implementation of the United States-Central America-Dominican Republic Free Trade Agreement Act, by virtue of which Honduras incorporated the provisions of said treaty in its domestic regime.

8. Legislative initiatives

The legislative initiatives being discussed in the legislature include the Information Technology and Electronic Government Framework Bill, the principal object of which is to establish a legal framework governing the application of new information and communication technologies in Honduras, and to promote economic and social development, citizen participation, national competitiveness and the efficiency and transparency of public administration, as well as to guarantee the legal security of electronic transactions and e-commerce.

(F) Nicaragua

Nicaragua's legislation has no specific law on e-commerce. Neither the Civil Code nor the Commercial Code mentions contracting via electronic media or the use of electronic media to take civil or mercantile action, including registry-related acts.

1. Electronic transactions and electronic signature

a. Commerce and finance

In the financial area, article 46 of the General Banks, Financial Institutions, Non-Banking Institutions and Financial Groups Act authorizes the use of electronic media to provide clients with monthly deposit account statements. Article 120 authorizes banks to use computer and microfilm systems in providing their services. Documents produced in these systems have full probative value, provided that the mechanisms used for their reproduction follow the resolutions and regulations of the Banking Superintendency, and that the documents are duly signed by an authorized official.

As regards securities market operations, the Capital Market Act permits the use of electronic media for various purposes. Article 61 authorizes the representation of securities in electronic accounting entries in connection with securities exchange contracts. Article 86 permits the use of electronic accounting entries to record investors' shares in different funds. Under article 121, securities issues charged to securitized funds must be represented exclusively by electronic accounting entries, and except in cases provided for in the law, the firms administering these funds must request admission in order to trade in an organized secondary market.

Similarly, article 137 permits the issuance of securities registered on the Registry of Securities of the Superintendency to be represented by electronic records known as intangible securities. In this connection, article 149 establishes that intangible securities are to be deemed such by virtue of being recorded in the corresponding accounting registry. The subscribers of physical securities have the right to register free of charge when the switch to electronic record-keeping is made. The Superintendency's Board of Directors has the authority to establish the general rules needed to ensure the fungibility of the securities for the purposes of compensation and settlement.

Under article 150, the transmission of securities, whether intangible or physical, deposited in a securities clearinghouse will take place via entry in the relevant accounting record. Article 163 provides for deposits in securities clearinghouses to be made through electronic recording of dematerialized securities.

b. Government

With regard to online government transactions, article 5 of the State Contracting Act obligates the State to plan, schedule, organize, conduct and supervise contracting activities in a manner such that its needs are met in a timely fashion and under optimal cost and quality conditions. It also requires procedures to be regulated and interpreted in a way that makes it possible to select the bids that best serve the public interest. This is to take place in a quantifiably rapid, rational and efficient way. The law also requires that regulations made to implement this law specify the form, timeframes and modalities applicable to the electronic communications media that are used as a supplementary and valid form of soliciting tenders in the State's contracting process.

Article 25 specifies the procedures for State contracting, namely: (i) public bidding; (ii) bidding by registry; (iii) restricted bidding; and (iv) quote-based purchasing. In restricted bidding, price quotes and other conditions surrounding the provision of the goods, works or services must be made in the context of a competitive process in which providers are invited to participate by written notice or e-mail, and compliance with this provision pursuant to the law and the corresponding regulations must be documented.

Article 63 of the regulations applying to State Contracting Act procedures requires agencies acquiring goods, works or services to explain their procedures via electronic media, with trustworthy records that make it possible to accurately identify messages' senders, recipients, time of sending, date of sending and content. Accordingly, the agency requesting bids may require bidders to provide e-mail addresses, fax numbers or other telematic addresses for receiving official communications. When these forms of communication are employed, the modality, date and hour of each communication must be documented by entries in the contracting file, and the entries must be signed by the employee responsible for them.

2. Consumer protection

The object of Law 182, the Consumer Protection Act, is to guarantee consumers optimal goods and services from their commercial relations, as well as amicable, fair and equal treatment by individual and collective public or private enterprises. Article 12 incorporates the basic consumer rights set forth in United Nations General Assembly Resolution 39/248, which deals with the Consumer Protection Guidelines, including the right to information and the right to safe products.
The law has no provisions directly referring to e-commerce, but online transactions are subject to rules guaranteeing consumers' right to clear information, in Spanish and presented with legible characters, that is accurate, complete and timely (and that includes information on the price, quality and guarantees associated with goods and services), and that observes the prohibition on misleading advertising and abusive clauses in membership contracts.

3. Privacy and data protection

As regards the protection of personal information, article 26 of the Nicaraguan Constitution enshrines the right of all persons to: (i) their and their family's private life; (ii) the inviolability of their residence, correspondence, and of communications of all types; (iii) due regard for their honour and reputation; and (iv) access to knowledge of all information regarding them contained in governmental records, as well as of the reasons and purpose for the possession of such information.

In this connection, the Public Information Access Act incorporates the right of habeas data, which article 4 defines as a guarantee of the protection of private personal data appearing in public or private files, records, databases and other technical media, the publishing of which is an invasion of personal/family privacy if the information published is sensitive personal information, or information regarding private or family life and affairs, when such information is in the possession of governmental entities defined as *sujetos obligados.* Habeas data guarantees all persons access to information that any public entity possesses concerning them, as well as the right to know why and for what purpose the entity possesses the information.

It also defines sensitive information, which consists of personal information that reveals a person's racial or ethnic origin; political views; religious, philosophical or moral convictions; political or union affiliations; state of physical or psychological health, or private life, regardless of the format in which the information is generated or stored. It defines private information as information consisting of personal information on an individual's private or family life, including health, race, political or religious preference, economic, social or family situation, or honour and reputation, as well as any personal information protected under the Constitution or by statutory law.

Article 15 of the law defines confidential public information as confidential banking information; trade, industrial, scientific or technical secrets belonging to third parties or to the State; intellectual property; and industrial, commercial or confidential information that the government has received as the result of a government requirement or procedure, without prejudice to the public nature of the Intellectual Property Registry, pursuant to relevant laws.

4. Intellectual property

With regard to intellectual property rights, article 127 of the Nicaraguan Constitution guarantees free and unconstrained artistic and cultural creation. It also stipulates that cultural workers are free to choose their forms and modes of expression, and that it is the State's duty to facilitate the means necessary for creating and disseminating their works and protecting their copyrights.

The Copyright and Related Rights Act protects literary, artistic and scientific works, as well as crafts objects and the work of artists, performers, producers of phonograms and broadcasting organizations. Computer programs are defined in article 2 as a set of instructions expressed in words, codes, graphics, designs or any other form, which, when put into an authorized reading device, are capable of making a computer, electronic device or the like produce information, carry out given tasks or obtain given results. Technical documentation and user manuals are also deemed to be part of such programs. Article 13 defines both source programs and object programs as literary works.

Article 14 also references databases, which it considers independent works. Article 31 permits reproduction of a published work for personal use, in the form of a copy of that work. However, it excludes reproducing all, or major portions of, numerical databases.

Reproduction is defined as including the making of one or more copies of a work, performance, phonogram or broadcast, either directly or indirectly, in any medium or form, including print, photocopies, recordings and permanent or temporary electronic storage. In connection with the related rights of artists, performers and broadcasting organizations, it defines the concepts of phonograms and videograms, and article 92 recognizes the right of producers of phonograms to authorize or prohibit the publication of their phonograms in any medium or by any procedure, wired or wireless, including broadcast.

The law includes civil and criminal sanctions for violations of the copyrights of artists, performers, producers of phonograms or broadcasting organizations. Article 111 sanctions the crime 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. Sanctions include prison sentences of two to three years and fines of up to 25,000 córdobas.

With regard to industrial property, under article 6 of Law 354, Patents for Inventions, Utility Models and Industrial Designs, mathematical methods or computer programs considered in isolation are not patentable inventions. The law protects business secrets that are held by a physical or juridical person under conditions of confidentiality, in order to prevent the information legitimately under said person's control from being disclosed to third parties, or from being acquired or used by third parties without consent in ways contrary to fair business practice.

Law 380, the Trademarks and Other Distinguishing Signs Act, establishes the requirements for the protection of trademarks, domain names, business names, denominations of origin and other distinguishing signs, and the terms under which such protection is provided. Article 27 defines when a brand is deemed to be in use, taking into account, among other things: (i) use of the sign in advertising, publications, business documents and written or oral communications, independent of the communication medium used; and (ii) adoption or use of the 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.

Under article 85, the owner or legitimate possessor of a widely-recognized distinguishing sign may request the courts to cancel or modify unauthorized registration of domain names or e-mail addresses that use the sign without authorization.

In regard to intellectual property rights, Nicaragua has ratified the following international documents:

- The WIPO Copyright Treaty (WCT) and Performances and Phonograms Treaty (WPPT)
- The Protocol to the Central American Agreement for the Protection of Industrial Property
- The United States-Central America-Dominican Republic Free Trade Agreement (CAFTA-DR)
- The Lisbon Agreement for the Protection of Appellations of Origin and their International Registration
- The Paris Convention for the Protection of Industrial Property (1883)
- The Berne Convention for the Protection of Literary and Artistic Works
- The Geneva Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of their Phonograms
- The Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations

- The Brussels Convention Relating to the Distribution of Programme-Carrying Signals Transmitted by Satellite
- The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) administered by the World Trade Organization (WTO)

5. Domain names

With regard to domain names, as well as the matters covered by Law 380 (the Trademarks and Other Distinguishing Signs Act), NIC NI (Nicaragua) (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 incorporated the Uniform Domain-Name Dispute-Resolution Policy of the Internet Corporation for Assigned Names and Numbers (ICANN), which conforms to international best practices. It recognizes the dispute resolution services provided thr ough the WIPO Arbitration and Mediation Centre.

6. Cybercrime

In the area of criminal law, article 192 of Law 641, which is the Nicaraguan Penal Code, provides for prison sentences of six months to two years 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. A sentence of one to three years may be imposed for disseminating or disclosing the content of such communication. A sentence of two to four years, and a fine equivalent to 300 to 500 days of basic wage may be imposed for the unauthorized act of promoting, facilitating, authorizing, financing, creating or marketing a database or computer record with information that can harm natural or juridical persons.

Article 198 provides for prison sentences of one to two years and a fine equivalent to 200 to 500 days of basic wage for the unauthorized use of computerized records of another, or unauthorized entry by any means in another's database or electronic files. Article 275 of the Code provides for prison sentences of two to four years or a fine equivalent to 300 to 600 days of basic wage for any person who, for benefit of self or of a third party, improperly 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, without the authorization of its legitimate holder or of an authorized user.

Article 247 provides for fines equivalent to 90 to 150 days of basic wage or a prison sentence of six months to two years or a prison sentence of six months to two years, plus a bar for the same amount of time from working in a job, occupation, post, industry or business related to the criminal conduct, for violating the law on this matter for the economic benefit of self or of a third party, by carrying out any of the following acts without written authorization of the rights holder:

(i) translating, arranging or otherwise transforming a work;
(ii) publishing a work or phonogram in any form, medium or by any procedure, either in whole or in part;
(iii) retransmitting a broadcast over any wired or wireless medium;
(iv) reproducing more copies than contractually provided for;
(v) distributing or communicating a work after the contract has ended;
(vi) falsely identifying the creator of a work;
(vii) carrying out any act to circumvent a technological measure that the rights holder has implemented to prevent unauthorized use of a work or phonogram;
(viii) manufacturing, importing, distributing and marketing, or providing mechanisms, devices, products or components, or offering installation services, to circumvent such technological measures;
(ix) altering or removing information regarding rights; or
(x) importing, distributing, marketing, renting or in any other way distributing works or phonograms whose rights information has been removed or altered.

Article 248 of the Code provides fines equivalent to 300 to 500 days of basic wage or a prison sentence of one to three years, plus a bar on working in a job, occupation, post, industry or business related to the criminal conduct, for using a copyright and related rights in violation of relevant law of the economic benefit of self or of a third party without authorization from the copyright holder, by any of the following acts:

(i) totally or partially reproducing a work or phonogram by any means, in any form or by means of any procedure;
(ii) distributing copies of a work or phonogram by sale, rental, public lending, importation or any other mode of distribution;
(iii) fixing the performance of an artist or performer; and
(iv) fixing a protected broadcast for later reproduction or distribution.

In addition, article 250 of the Code provides fines equivalent to 300 to 500 days of basic wage or a prison sentence of one to three years, plus a bar for the same amount of time from working in a job, occupation, post, industry or business related to the criminal conduct, for illegally manufacturing, distributing or selling mechanisms or systems that permit or facilitate the unauthorized removal of technical devices used to prevent the reproduction of computer programs.

7. Taxes and customs

In the tax area, article 34 of the Tax Code authorizes payment of taxes via electronic media or systems, provided that the taxpayer is realistically able to use such means. Article 81 authorizes taxpayers to keep accounting records and issue invoices electronically, following the standards set by the Tax Administration. Article 82 authorizes taxpayers to carry out their procedures via the internet and other previously regulated electronic systems. Article 83 stipulates that text submitted by automated means will be valid only upon official documentation of its receipt by the Tax Administration.

Article 84 of the Tax Code permits the use of electronic media for notification of administrative actions, provided that taxpayers and/or their representatives are formally notified by the Tax Administration through ordinary communications systems, computerized means, electronic media or the like, and provided that the medium used allows for confirmation of receipt. Article 86 permits taxpayers who have explicitly agreed to electronic notification to be notified by sending notice to their electronic files. In addition, under article 90, means of proof dependent on technological advances can be used if they are verifiable, technically supported and capable of providing certainty regarding the facts. Examples of this include direct voice recordings, videos, cell phone messages, e-mails and/or transactions via computer networks.

Article 148 provides broad authority for oversight and investigation to legal auditors or inspectors, so that, among other things, they can require taxpayers and their representatives to provide any information stored on magnetic media or obtained via the internet. Receipt of information on electronic storage media is also permitted.

In the customs area, Nicaragua has adopted CAUCA, RECAUCA and CAFTA-DR, as detailed below.

8. Legislative initiatives

The principal legislative initiatives being reviewed by the National Assembly include the Electronic Signature Bill, the objective of which is to regulate the use of electronic signatures in legal instruments and contracts made between natural or juridical persons in electronic media.

(G) Panama

The most important legislation for the development of e-commerce in Panama is Law 51 of 22 July 2008, which defines and regulates electronic documents and electronic signature, and allows the provision of technological storage services for documents, as well as electronic signature certification services. In another context (Law 51), the law adopts provisions for the purposes of developing e-commerce.

This law incorporates various elements of the UNCITRAL model laws on e-commerce and electronic signature, as well as elements of the European Commission Directives on e-commerce, electronic signature and remotely handled direct marketing. Under the law, the entity authorized to supervise providers of certification and technological storage services is the Directorate of Electronic Commerce.

Law 51 establishes regulations on a variety of aspects of electronic transactions between private parties and of electronic transactions involving the government. It also includes a number of consumer protection measures covering e-commerce operations, with stipulations regarding the responsibilities of commercial service providers using the internet, including providers of intermediation services. These measures are detailed in specific paragraphs of the law.

On the international front, Panama has signed the United Nations Convention on the Use of Electronic Communications in International Contracts (CUECIC), but has not yet ratified it.

1. Electronic transactions and electronic signature

The object of law 51, as stated in article 1, is to establish a regulatory framework for the creation, use and storage of electronic documents and electronic signatures, as well as for the registering and oversight of providers of technological storage services for documents and providers of electronic signature certification services in Panama's national territory.

It also 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, the obligations and responsibilities of entities providing commercial services via the internet (including those acting as intermediaries for the transmission of contents through communications networks), 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.

The law defines the functions and responsibilities of providers of certification services, as well as the mandatory content of digital certificates and electronic signatures. It also regulates the obligations of providers of electronic document storage services.

In situations where the law requires that information be put in the form of a written document, article 4 makes legal instruments and contracts generated in electronic form or adapted to it valid, legally effective and binding. Under article 7, electronic documents are admissible as evidence and have the same probative weight as paper documents. The trustworthiness of the way 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.

Article 8 gives electronic signatures the same value, in relation to information in electronic form, as written signatures have in relation to information in paper documents.

Article 17 recognizes the validity of certificates issued by providers of foreign electronic signature certification service providers, as long as:

(i) the certificates are recognized under agreements with other countries;
(ii) they are issued by certification service providers that are officially endorsed, in their country of origin, by institutions analogous to the Directorate of Electronic Commerce;
(iii) there is accreditation that the certificates were issued by a certification service provider that meets the minimum standards of the Directorate of Electronic Commerce.

With regard to technological document storage, article 44 states that, in cases where the law requires certain documents, records or information to be presented and preserved in their original form, electronic documents are satisfactory if there is accreditation that, among other things:
(i) there is a reliable guarantee that the integrity of the information has been preserved from the moment when it was first generated in its definitive form as an electronic document;
(ii) the information can be presented to the person indicated;
(iii) any information permitting determination of the electronic document's origin and destination, as well as of the date and time of its sending or receipt, has been preserved.

Article 45 gives documents stored technologically, pursuant to the law, as well as film, reproductions and certifications of them that have been duly authenticated, the same legal force as the original documents.

Article 51 recognizes the legal validity of documents legally stored in other countries, provided that:

(i) they are recognized by virtue of agreements with other countries;
(ii) they have been technologically stored by providers of such services which have been officially endorsed, in their country of origin, by institutions analogous to the Directorate of Electronic Commerce;
(iii) there is accreditation that such electronic documents were collated with their originals in the country where they were issued, by the Panamanian Consul, or by the consul of a friendly nation, or by any authority with the capacity to confer public trust;
(iv) there is accreditation that such documents were issued by a technological storage services provider that meets the minimum standards of the Directorate of Electronic Commerce.

With regard to the issue of limited liability, article 88 of Law 51 defines cases in which such limitation applies to network operators and access providers that transmit data provided by a user of their services and have not originated a transmission or modified or selected its contents or addressee(s).

Under the law, modification does not refer to strictly technical manipulation of the files containing the data during the transmission of such files. Transmission and provision of access are defined as including automatic, provisional and temporary data storage, provided that it is only used to facilitate transmission through a communications network and that its duration does not exceed that permitted by the law's technical regulations.

Article 89 defines the cases in which there is limited liability for commercial service providers that operate via the internet, where such providers make temporary copies of data requested by users solely for the purpose of improving subsequent transmission of that data to other recipients requesting them.

Article 90 sets forth the conditions under which liability is limited for providers of data warehousing or storage services, provided that they lack effective knowledge that the activity or information stored is illicit or is detrimental to the assets or rights of a third party with a relevant claimable right. It also recognizes the validity of procedures to detect and remove contents of a communications network that a provider of data warehousing or storage services employs pursuant to regulations, voluntary agreements and other means of effective knowledge that may be established.

In addition, article 91 defines cases in which there is limited liability for a service provider that provides links to search contents or instruments.

a. Commerce and finance

Article 78 of Law 51 establishes that the provision of commercial services via the internet by a firm based in another State shall take place under the regime of unrestricted provision of services, and on the basis of criteria established in international agreements. However, firms that promote their services and conduct commercial transactions in Panama via the internet must comply with Panamanian technical requirements and other legislative and regulatory obligations.

Law 51 amends various articles of the Commercial Code. The principal changes affect provisions relating to rules governing commercial activity in article 6 of the Code. Under the Code, Panamanian law is applicable to such activity as regards the essence and downstream or immediate effects of the obligations deriving from it, except where there has been agreement to the contrary or where clear notice to the contrary is in effect, and as regards the way in which the obligations are met, unless other stipulations have been agreed to or the proposing party's offer explicitly applies to a consumer in Panamanian territory, in which case only Panamanian laws and regulations apply.

The law also stipulates that, with regard to legal instruments and their external formalities and form, the laws in the place in which documents are executed govern, except where the law explicitly provides otherwise. As regards the legal capacities of the contracting parties, the laws of their respective countries apply, unless one of the parties is a consumer in Panamanian territory, in which case only Panamanian law and regulations apply.

Article 71 requires merchants to keep accounting records, which may take the form of electronic documents. In cases of commercial operations conducted through the internet, merchants are obliged to document the terms of the offer or provide electronic invoices. The article also authorizes juridical persons to maintain, in electronic form, registries and records of equity shares.

Under article 195 of the Code, the validity of mercantile contracts does not depend on special forms**,** except where the law requires that they be registered as documents of public record or that they comply with other formalities.

Article 196 stipulates that when the law requires a contract to be made in written form, either physically or in equivalent electronic form, the requirement also applies to any essential modification of the contract. It further recognizes the sufficiency of mechanical or technological forms of signature, provided that the legal formalities established for their validity have been observed.

Article 201 stipulates that a party proposing a contract to another and setting a time limit for its acceptance is bound by the offer until the specified time has elapsed, whether or not the two parties have met face to face. When transactions conducted via electronic communication media are involved, the proposing party must indicate the natural or juridical person in whose name the transaction is occurring, and must inform the recipient clearly, comprehensibly and unequivocally of the mechanisms that will be used to determine and establish the date and hour at which the contract or transaction will be deemed executed.

Under article 205A, acceptance of the offer, and confirmation thereof, are deemed received when documentation of the fact becomes available to the parties. It is not necessary to confirm receipt of the acceptance of an offer if both contracting parties so agree and neither is a consumer.

Article 245 of the Commercial Code stipulates that when mercantile law requires that a contract be in written form, no other proof of its existence is admissible, and in the absence of a written contract in physical form or an electronic equivalent, the contract is deemed void.

Law 51 amends article 1103 of the Civil Code, which stipulates that contracts and obligations can be accredited only on the basis of written proof, whether physical or electronic. In addition, it amends article 873 of the Judicial Code to recognize the probative value of original documents in physical form or in their electronic equivalent, provided that the technological storage of the document has met the requirements of the law.

b. Government

Under article 13 of Law 51, the State may use electronic signatures internally and in its relations with private parties, pursuant to the provisions of this law and the conditions set forth in regulations pertaining to the several branches of government. This article also stipulates that private parties who conduct relations with the State via electronic media must use electronic signatures issued by a provider of electronic signature certification services registered with the Directorate of Electronic Commerce. In addition, article 50 of the law authorizes the State to use technological document storage internally and in its relations with private parties, pursuant to this law and the conditions set forth in regulations pertaining to the several branches of government.

2. Consumer protection

With regard to consumer protection, article 49 of the Constitution recognizes and guarantees the right of all persons 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.

Article 49 also mandates that the law establish the mechanisms needed to guarantee these rights, to promote consumer education and protection, to ensure indemnification for damages caused, and to punish violations of these rights.

Law 45 of 31 October 2007 develops the above-mentioned Constitutional principles and incorporates basic consumer rights pursuant to United Nations General Assembly Resolution 39/248, which deals with the Consumer Protection Guidelines, including consumers' right to information and to safe products.

In the e-commerce area, article 74 of Law 51 authorizes the use of seals of trust to promote the use of the internet as a secure medium for offering and obtaining commercial goods and services. This is without prejudice to other legal provisions on specific activities or matters, permitting all natural and juridical persons, as well as the Directorate of Electronic Commerce and other public or private entities, to grant such seals of trust to firms offering commercial services over the internet if they meet the relevant legal requirements.

Article 92 incorporates codes of conduct in Panamanian law in the capacity of self-regulatory instruments governing, among other things, procedures to detect and remove illicit content, and to protect users of e-mail from unsolicited commercial e-mail, as well as providing extrajudicial procedures to resolve disputes arising from the provision of commercial services via the internet. Article 93 authorizes service providers, consumers and users to participate in developing these codes, the principal objectives of which must include protecting minors and human dignity, and addressing relations with consumers, as well as the issue of undesired e-mail.

Article 83 of Law 51 authorizes the relevant authorities to request the Directorate of Electronic Commerce to adopt the measures needed to interrupt the provision of a commercial service via the internet if it is detrimental to the public health or to consumers, even if the service is based in another country.

Measures to limit unsolicited commercial communications include article 85 of Law 51, which requires all commercial communications to be clearly identifiable as such, and to identify the natural or juridical person in whose name they are being sent. The addressee must also be given a way to prevent future communications from the sender. A provider of commercial services via the internet who intentionally resends a message, sends a new message and/or uses another e-mail address to re-contact an addressee who has asked not to be contacted is guilty of a felony.

Commercial communications sent via e-mail must include the word "advertising" or some other term that clearly identifies the message's intention, in such a way that the addressee can recognize the nature of the e-mail even before opening it or accessing its text.

In addition, article 86 prohibits utilizing users' information without their authorization. If the recipient of a service is required to provide an e-mail address during the process of contracting for or subscribing to it, and the provider intends to use the address later to send commercial communications, the provider must make this intention known to the client and request the client's consent before the contracting process has concluded. The user may at any time revoke consent for commercial communications by simply notifying the sender.

3. Privacy and protection of personal information

Article 29 of the Panamanian Constitution 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.

Article 42 gives all persons the right to access personal information on themselves contained in public and private databases, and to demand the correction and protection, as well as the removal, of such information, in conformity with the law. Such information can only be collected for specific purposes, with the consent of the person to whom it pertains, or by authorization of a governmental entity pursuant to the law.

Article 44 of the Constitution 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. The law must regulate which courts can hear habeas data actions, and such actions must take the form of summary hearings without the need for an attorney.

Article 106 of Law 51 establishes a special regime to guarantee the inviolability of the information deposited in databases as backup for operations in foreign countries or jurisdictions by private or public enterprises, including State and international organizations.

Article 108 makes it a matter of public domain and of public policy that the information contained in data backups by foreign firms or international entities in databases in Panama can in no case, and for no cause, be the object of precautionary or documentary measures for the handling of said information by judicial, administrative or tax authorities.

In the area of banking confidentiality, article 110 of Executive Decree 52-2008, which adopts intact the text of Decree Law 9 of 26 February 1998, amended by Decree Law 2 of 22 February 2008, stipulates that information relating to a bank's individual clients obtained by the Superintendency of Banks in Panama in the exercise of its functions shall be kept strictly confidential, and disclosed only upon request by an authorized government entity during the course of a criminal proceeding pursuant to current legal provisions.

Article 111 of the decree stipulates that only with consent may banks disclose information relating to their clients or operations. This is in contrast to cases where information is being requested by a government entity in conformity with the law, and cases where the information must be provided to comply with laws to prevent laundering of assets, financing of terrorism and other related crimes, etc.

Law 24 of 2002, amended by Law 14 of 2006, contains various measures relating to the management of information regarding consumers' credit history.

4. Intellectual property

Article 53 of the Panamanian Constitution gives all authors, artists and inventors exclusive ownership over their works and inventions for the duration and in the manner established by the law.

In the industrial property rights area, article 14 of Law 35 of 10 May 1996, amended by Law 1 of 5 January 2004, declares that neither mathematical methods nor computer programs in isolation are considered inventions eligible for patent protection.

This law also protects industrial and commercial secrets, which article 83 defines as all information of industrial or commercial use held by a natural or juridical person under conditions of confidentiality, and giving its possessor a competitive or economic advantage over third parties in the context of economic activity, and in respect to which information said person has employed appropriate means or systems to preserve its confidentiality and restrict access to it. Under article 85, secrets may be contained in electronic media. With regard to trademarks, law 35 has no stipulations regarding internet use or use of domain names.

In the copyright area, Law 15 of 8 August 1994 approved the Copyright and Related Rights Act, articles 7 and 8 of which stipulate that computer programs and databases are subject to protection by copyright. With regard to the related rights of artists, performers and broadcasting organizations, this law defines the concepts of phonogram and videogram, and recognizes the right of publication via any medium.

On the international front, in the intellectual property rights area, Panama has ratified:

- The WIPO Copyright Treaty (WCT) and Performances and Phonograms Treaty (WPPT)
- The Protocol to the Central American Agreement for the Protection of Industrial Property
- The United States-Central America-Dominican Republic Free Trade Agreement (CAFTA-DR)
- The Lisbon Agreement for the Protection of Appellations of Origin and their International Registration
- The Paris Convention for the Protection of Industrial Property (1883)
- The Berne Convention for the Protection of Literary and Artistic Works
- The Geneva Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of their Phonograms

- The Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations
- The Brussels Convention Relating to the Distribution of Programme-Carrying Signals Transmitted by Satellite
- The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) administered by the World Trade Organization (WTO)

5. Domain names

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

6. Cybercrime

Articles 61 and 110 of Law 51 include specifications of crimes. Article 61 establishes criminal liability for altering or adulterating technologically stored documents, pursuant to the Penal Code's provisions regarding crimes against the public trust, and without prejudice to civil or administrative liability that may result from such criminal activity. Under article 10, the improper disclosure of technologically stored information is equivalent to the crime of disclosing business secrets, as described in Law 14 (Penal Code).

Law 14, Penal Code, defines various crimes connected with illicit access to computer systems, as well as the interception of electronic communications, the illicit disclosure of industrial secrets and the unauthorized production of works protected by copyright and related rights.

Article 283 of Law 14 provides for two to four years of prison for improper entry to or use of databases or computer networks or systems. Article 284 provides for two to four years of prison for improperly stealing, copying, using or modifying data in transit or data contained in a database or computer system, or interfering with, intercepting or impeding the transmission thereof. Sentences are increased Article 286 increases sentences by one third or one sixth for crimes committed against data in computer-system databases 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.

In addition, article 286 stipulates that if the conduct described in articles 283 to 285 are committed by the person overseeing or responsible for the database or computer system, or by a person authorized to access it, or if the person carrying out the act uses privileged information in committing the crime, sentences are to be increased by between one third and one sixth.

For interfering with communications, article 162 provides for one to three years of prison or an equivalent fine in days of basic wage, or weekend arrest, when the person engaged in the act takes or improperly discloses the content of a letter or e-mail not addressed to him.

Article 163 provides for sentences of two to four years of prison or an equivalent fine in days of basic wage, or weekend arrest, for taking, destroying, replacing, hiding, losing, intercepting or blocking a letter or e-mail, with sentences increased by one sixth if the information is published or disclosed. If the person committing the crime is a public servant or an employee of a telecommunications firm, the sentence increases to three to five years of prison, with an additional one sixth that amount if the information is published or disclosed.

In relation to the improper disclosure of industrial or business secrets, article 266 provides for four to six years of prison for taking or using information contained in an industrial or business secret without the consent of the person possessing it or of its authorized user, in order to obtain economic benefit for self or for a third party, or in order to cause damage to the person holding the secret or to its authorized user. Article 267 provides for two to four years of prison for unjustifiably disclosing an industrial or business secret if the person carrying out the act is aware of its confidentiality, if the crime is committed for the

purpose of economically benefiting self or a third party, or to cause harm to the person holding the secret or to its authorized user.

With regard to copyright and related rights, article 256 provides for one to three years of prison or a fine equivalent to 200 to 400 days of basic wage for publicly communicating a duly protected work in any form or by any procedure, in either its original or a converted form, either in whole or in part, without the authorization of the rights holder or in violation of the limits permitted by the relevant laws. Article 258 provides for four to six years of prison for distributing, exporting, assembling, manufacturing, selling, renting or in any other way circulating an illicit reproduction of a protected work, or for reproducing, copying or modifying it industrially, by laboratory means or through automated processes, without the authorization of the rights holder or in violation of the limits permitted by the relevant laws.

Article 259 provides for one to three years of prison or a fine equivalent to 200 to 400 days of basic wage for reproducing or copying, without authorization, the performance of an artist or performer, a phonogram, videogram, computer program or broadcast in whole or in part, or importing, storing, distributing, exporting, selling, renting or in any other way circulating such reproductions or copies.

Article 260 sanctions the manufacture, assembly, modification, importation, sale or offering for sale, rental, or circulating, for illicit purposes, of decoders or any other artefact, equipment, device or system designed exclusively to connect, receive, remove, impede, deactivate or circumvent the technical devices that authorized distributors or concessionaires of signal-carrying programmes, sounds, images, data or any combination of these have or have installed for the protection or reception of same. Corresponding sentences are two to four years of prison.

7. Taxes and customs

Decree Law 1 of 13 February 2008 created the National Customs Authority and established various provisions by virtue of which the use of electronic media for customs procedures is acceptable. The criteria for the characteristics of the technological platform are set forth in the corresponding body of regulations.

With regard to taxation, Law 51 of 2008 recognizes the legal validity of electronic invoices, defined in article 2 as electronic documents documenting the sale of goods or provision of services by a commercial service through electronic media, in such a way as to make the commercial operations carried out subject to taxation. In addition, the Tax Code and Resolution 201-2969 of 15 August 2007, issued by the Directorate of Internal Revenue of the Ministry of Economy and Finance, authorize the submission of sworn statements by electronic media.

8. Legislative initiatives

The principal legislative initiatives being debated in the National Assembly include bill 15 of 18 September 2009, which sets forth standards for the preservation, protection and provision of the data of users of telecommunications services.

III. TOWARDS REGIONAL HARMONIZATION

The multiplicity of international, regional and subregional organizations and treaties in which the Central American countries participate has led to a proliferation of normative instruments and national policies, as demonstrated in section II, above. By way of clarifying the different international strategies and instruments for harmonizing the region's cyberlegislation, the present section describes existing laws and regulations in Central America, as well as the main treaties that regional institutions have promoted to guide present and future activities aimed at achieving greater economic and political harmonization through Central American regulatory harmonization.

A) Normative report for the region

1) e-LAC 2007 and e-LAC 2010 Regional Plans[5]

The e-LAC 2007 and e-LAC 2010 Regional Plans coordinated by ECLAC are a cornerstone for the regional harmonization of public policies and regulations. Goal 25 of the e-LAC 2007 Plan is to "Establish subregional working groups to promote and foster policies for harmonizing norms and standards, with the aim of establishing legislative frameworks that merit trust and offer security at both the national and regional levels, paying special attention to legislation on the protection of privacy and personal data, cyber-crime and ICT crime, spam, digital or electronic signatures, and electronic contracts as a framework for the development of the information society."

The participation of the Observatory for the Information Society in Latin America and the Caribbean (OSILAC), sponsored by ECLAC and the Institute for Connectivity in the Americas (ICA) at the Canadian Government's International Development Research Centre (IDRC), facilitates assessment and action by generating and processing statistical information that, among other things, makes it possible to monitor advances in public policy related to the development of ICT at the regional, subregional, national and local levels.

2) Organization of American States[6] – Inter-American Telecommunication Commission (CITEL)[7] and the Network of Electronic Government of Latin America and the Caribbean (GEALC)[8]

[5] Available at: http://www.eclac.org/socinfo/elac/.

[6] The members of the OAS are: Antigua and Barbuda, Argentina, the Bahamas, Barbados, Belize, the Plurinational State of Bolivia, Brazil, Canada, Chile, Colombia, Costa Rica, Dominica, Ecuador, El Salvador, United States, Grenada, Guatemala, Guyana, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, the Dominican Republic, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname, Trinidad and Tobago, Uruguay and the Bolivarian Republic of Venezuela. See: http://www.oas.org/main/spanish/.

[7] CITEL is the OAS body specializing in telecommunications. See: http://www.citel.oas.org/citel_e.asp.

[8] The GEALC network was created by the OAS Executive Secretariat for Integral Development and the Institute for Connectivity in the Americas (IDRC/ICA) in 2003, in order to promote horizontal cooperation among the countries of Latin America and the Caribbean, and to facilitate the sharing of solutions and experts among them. See: http://www.redgealc.net/.

The efforts of the Organization of American States (OAS) and the Inter-American Telecommunication Commission (CITEL) on connectivity,[9] network security and cybercrime have influenced the development of legal frameworks in Panama and the Dominican Republic.

Participation in the Network of Electronic Government of Latin America and the Caribbean (GEALC), which is sponsored by the OAS, has promoted the integration of one-stop shops in Costa Rica, El Salvador, Guatemala and the Dominican Republic.

3) Central American Integration System (SICA)

On 13 December 1991, the Central American Integration System (SICA) was created upon the signing of the Tegucigalpa Protocol, which amended the 1962 Charter of the Organization of Central American States (ODECA). SICA serves as the institutional framework for Central American regional integration and was created by the States of Belize, Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua and Panama.

The Dominican Republic participates as an Associated State, with México, Chile and Brazil being Regional Observers, and Taiwan Province of China, Spain and the Federal Republic of Germany serving as Extraregional Observers. The SICA General Secretariat is headquartered in El Salvador.

The Protocol to the General Treaty on Central American Economic Integration, which was signed on 29 October 1993, commits the parties to the voluntary, gradual, complementary and progressive creation of the Central American Economic Union. For this purpose, the Economic Integration Subsystem was created, along with its technical and administrative body, the Central American Secretariat for Economic Integration (SIECA), headquartered in Guatemala.

The basic objective of SICA is to promote Central American integration. Accordingly, it has articulated the following goals: (i) to achieve a regional system of welfare and economic and social justice for the Central American peoples; (ii) to achieve an economic union and strengthen the Central American financial system; (iii) to strengthen the region as an economic block in order to ensure its successful insertion in the international economy; and (iv) to build the Central American Integration System on an institutional and legal foundation of mutual respect between the member States.

Among the activities of SICA are collaboration in various cooperation forums, including: (i) the Forum for Korea-Central America Cooperation; (ii) the Forum for Japan-Central America Cooperation; (iii) the Forum for China-Central America Cooperation; (iv) the Forum for European Union-Central America Cooperation; (v) the Forum for CARICOM-Central America Cooperation; (vi) the Vienna Forum; (vii) the India Forum; and (viii) the Mesoamerican Cooperation Programme, as well as interaction with the Latin American Integration Association (ALADI), the Andean Community (CAN)[10] and the Southern Common Market (MERCOSUR).[11]

4) Central American Customs Union

In order to advance the region's economy, improve the living conditions of its inhabitants, establish a Central American Common Market, create a sound free trade zone and establish a Central American Customs Union, as well as to establish a common external tariff in the context of a subregional economic union, the governments of Guatemala, El Salvador, Honduras, Nicaragua and Costa Rica signed the General Treaty on Central American Economic Integration. On 13 December 1963 they promulgated the

[9] The Connectivity Agenda for the Americas, presented at the International Telecommunications Union (ITU) World Telecommunications Development Conference in Istanbul, Turkey, in March 2002.
[10] See: http://www.comunidadandina.org/.
[11] See: http://www.mercosur.int/msweb/portal%20intermediario/es/index.htm.

Central American Uniform Customs Code (CAUCA), which includes the basic provisions of a common legislative framework for customs, as a basis for organizing customs services and regulating their administration

CAUCA provides the foundation for the Central American Customs Service, which is to be organized in a way that ensures technical and administrative efficiency in customs operations involving merchandise, whether exports (final or temporary exports, or re-exports) or imports (commercial, non-commercial and temporary imports, as well as re-imports and entering goods that are to remain in international transit). The Code sets forth the authorities and responsibilities of CAUCA.

As a corollary to CAUCA, the Central American Customs Union adopted the CAUCA Regulations (RECAUCA). These include the provisions of the Central American Uniform Customs Code, and are consistent with the WTO General Agreement on Tariffs and Trade (GATT). There is also provision for interaction of authorized economic operators[12] with the World Customs Organization (WCO) and other international entities, in order to facilitate and optimize the security of the international logistics chain.

Among the principal authorities that RECAUCA confers on the Customs Service, which operates the Central American Customs System are:

(i) requiring and verifying compliance with the elements that determine customs obligations, such as the nature, characteristics, tariff classifications, origin and customs value of merchandise, and the other duties, requirements and obligations associated with merchandise that enters, remains in or exits, and the means of transport used within, the customs territory;
(ii) requiring and verifying payment of taxes;
(iii) developing and enforcing customs procedures, as well as proposing modifications of the regulations to adapt them to technical and technological changes, as per the demands of international trade and criteria of simplicity, specificity, uniformity, effectiveness and efficiency;
(iv) requiring the electronic transmission of information for application of the different customs regimes and operations; and
(v) requiring auxiliary entities, importers, exporters, producers, declarants and third parties related to these to submit accounting books, attachments, files, accounting records and inventory control and management records, other tax- and customs-related information, and magnetic or other similar media used to back up or contain the information, pursuant to the terms set forth in customs legislation.

A number of sections of the regulations also recognize the legal validity of online commercial transactions, as well as tax and customs transactions, provided that they employ digital signatures backed by digital certification. Chapter VIII, which deals with the use of computer systems and digital signature certification service providers, is particularly relevant, since it establishes measures to promote the technical and legal security of electronic communications, as well as of the digital information exchanged between authorized operators, the Customs Service and the auxiliary entities participating in customs procedures.

RECAUCA incorporates a number of principles of the UNCITRAL model laws on e-commerce and digital signature, such as the functional equivalence of signed paper documents and digitally signed electronic documents, and mutual recognition of digital signatures issued by certification entities in different countries. However, it uses its own terminology in place of the basic formulation of concepts articulated in the model laws. It employs the term “electronic document” in place of “data message”, and refers to

[12] The World Customs Organization defines the term “authorized economic operator” as “a party involved in the international movement of goods in whatever function that has been approved by or on behalf of a national Customs administration as complying with WCO or equivalent supply chain security standards. Authorised Economic Operators include inter alia manufacturers, importers, exporters, brokers, carriers, consolidators, intermediaries, ports, airports, terminal operators, integrated operators, warehouses and distributors”.

signers rather than *subscribers*. Also, it uses the terms "electronic signature" and "digital signature" interchangeably, without specifying the legal differences relating to the reliability of the methods behind each.

Under RECAUCA, the computer systems used in customs procedures must ensure the privacy, confidentiality, non-deniability and integrity of data and documents that are transmitted and stored, as well as the authenticity of the entity issuing them, and of the users of the Customs Service information systems. Therefore, customs agents, special customs brokers and depositories must employ confidential user names and passwords provided by the Customs Service. They must also use private and public keys provided by a certifier authorized by the Customs Service for transmitting statements, electronic documents and electronic or digital signatures.

Authorized economic operators must meet international logistics chain security standards and employ appropriate information technology security measures to protect the computer system from unauthorized intrusion, as well as take any necessary measures to ensure the security and proper preservation of records and documents relating to customs operations subject to oversight.

The regulations also provide that data and documents transmitted through computer systems may be certified through entities specializing in the issuance of digital certificates that guarantee the authenticity of the messages used to exchange data. Such entities must be authorized by the head of the Customs Service, or by the entity that administers and supervises the certification system of the State Party, pursuant to national legislation on digital signatures.

The elements of RECAUCA that are most important for the region's regulatory harmonization include the establishment of a Central American Commission on Electronic or Digital Certification, an entity responsible for formulating the general operational policies of the electronic or digital signature system for Central American customs services. Such policies include those governing the structure, conditions and procedures involved in the issuance, suspension, revocation and expiration of certificates and electronic or digital signatures issued by authorized certification entities, pursuant to the conditions established, through the Commission, by the countries' customs services.

The regulations recognize, as a general principle, that customs regimes are formalized through the electronic transmission of data to the Customs Service; thus, the submission and acceptance of merchandise declarations are handled in that form. Matters connected with the application of risk criteria, the results of immediate verification, release authorizations and other procedures involved in customs clearance are also handled electronically.

The regulations require that customs duties be paid through electronic funds transfers, using financial-system banks authorized by the Customs Service or other relevant authority, with appropriate notification to said authorities.

RECAUCA provides for the creation of a regional database, with information provided by customs authorities and authorized customs operators. It also lays the foundation for implementing an electronic risk management system, as well as contingency procedures to ensure the continuity of customs services.

The regulations permit electronic auction mechanisms through the Customs Service's auction web page. Parties interested in participating in auctions must register as users and employ passwords to access the site. The procedures allow participants to appeal decisions of the authority, notice of which may be sent electronically.

5) United States-Central America-Dominican Republic Free Trade Agreement (CAFTA- DR)

The governments of Costa Rica, the Dominican Republic, El Salvador, Guatemala, Honduras, Nicaragua and the United States signed this treaty to establish a free trade area, as provided for in article XXIV of the 1994 General Agreement on Tariffs and Trade (GATT) and article V of the General Agreement on Trade in Services, both of which are administered by the World Trade Organization (WTO). Although Panama is not a party to CAFTA-DR, it has signed a Trade Promotion Agreement with the United States, the content of which is nearly identical to that of CAFTA-DR.

The guiding principles of CAFTA-DR are transparency and most-favoured nation treatment. The treaty's objectives include:

(i) encouraging the expansion and diversification of trade between the parties;
(ii) eliminating trade barriers and facilitating the cross-border circulation of goods and services between the parties' territories;
(iii) providing appropriate and effective protection for, and enforcement of, intellectual property rights in each party's territory;
(iv) establishing guidelines for bilateral, regional and multilateral cooperation, in order to expand and improve the treaty's benefits.

Chapter V of the treaty, entitled "Customs Administration and Trade Facilitation", provides for measures to encourage the automation of customs procedures, in order to streamline the clearance of merchandise by:

(i) facilitating the electronic submission and processing of information and data prior to arrival, thus making it possible to clear merchandise upon arrival;
(ii) using electronic or automated procedures to analyse risk and identify high-risk targets;
(iii) working to develop compatible electronic procedures among the parties' customs authorities, in order to facilitate the exchange of international trade data between governments; and
(iv) working to develop a set of processes and common data elements, in conformity with the WTO Customs Data Model and other related WTO recommendations and guidelines.

The treaty includes a chapter specifically dealing with e-commerce (chapter XIV), which the parties consider to be a driver of economic growth, and which should therefore be exempt from obstacles that prevent its use and development. The treaty also establishes the applicability of WTO rules with regard to measures affecting e-commerce. It allows for the electronic provision of services, to which the relevant provisions of chapters V (Investment), VI (Cross-Border Trade in Services) and XII (Financial Services) are to be applicable, and which will be subject to any exceptions or contrary measures established in the treaty.

CAFTA-DR includes the following definitions as related to e-commerce:

- *Electronic media:* refers to the use of computerized processing;
- *Carrier medium:* any physical object capable of storing digital codes that constitute a digital product by any method currently known or subsequently developed, by which a product may be directly or indirectly received, reproduced or communicated, including optical media, diskettes and magnetic tape.
- *Digital products:* computer programs, text, video, images, sound recordings and other digitally coded products.[13]
- *Electronic transmission / electronically transmitted:* transfer of digital products via any electromagnetic or optical medium.

The treaty prohibits the parties from imposing customs duties or tariffs on digital products or imposing other charges in connection with importing or exporting digital products via electronic transmission. It also provides that customs tariffs are to be determined based on the customs value of the imported carrier medium that incorporates the digital product, regardless of the actual cost or value of the carrier medium, and independent of the cost or value of the digital product stored in the carrier medium.

With regard to international cooperation on e-commerce issues, the parties recognize the global nature of e-commerce, and propose to:

[13] By way of clarification, digital products do not include digitized representations of financial instruments.

(i) work together to overcome obstacles to the use of e-commerce by small and medium-sized enterprises;
(ii) share information and experiences regarding e-commerce laws, regulations and programmes, including those designed to address issues of data privacy, consumer confidence in e-commerce, cybersecurity, electronic signature, intellectual property rights and e-government;
(iii) work to maintain cross-border information flows as an essential element in promoting a dynamic e-commerce environment;
(iv) encourage the private sector to adopt self-regulatory measures, including codes of conduct, model contracts, guidelines and enforcement mechanisms that encourage e-commerce; and
(v) participate actively in hemispheric and multilateral forums to promote the development of e-commerce.

Chapter XV (Intellectual Property Rights) sets forth the minimum legal framework that the parties are to incorporate in their national legislation to protect intellectual property rights. The treaties that the parties are to ratify include:

- The WIPO Copyright Treaty (1996)
- The WIPO Performances and Phonograms Treaty (1996)
- The Patent Cooperation Treaty, as revised and amended (1970)
- The Convention Relating to the Distribution of Programme-Carrying Signals Transmitted by Satellite (1974)
- The Trademark Law Treaty (1994)
- The Patent Law Treaty (2000)
- The Protocol to the Madrid System for the International Registration of Marks (1989)
- The TRIPS Agreement and intellectual property agreements made or administered under the auspices of the World Intellectual Property Organization (WIPO) of which they are a part.

Among the novel aspects of the treaty are the presence of sound and olfactory marks. The parties also commit to provide, to the extent possible, an electronic system for trademark applications, processing, registration and maintenance. The treaty establishes a commitment to develop, wherever possible, an electronic database available to the public, showing both trademark applications and trademarks that have been granted. It also provides for the possibility of making notifications via electronic media.

With regard to domain names, CAFTA-DR stipulates that, in order to combat cyberpiracy of trademarks, all parties will require entities administering top-level country domains to include appropriate dispute resolution procedures based on the principles set forth in the Uniform Domain-Name Dispute-Resolution Policy of the Internet Corporation for Assigned Names and Numbers (ICANN).

The treaty also stipulates that all parties must require the entities administering their top-level country domains to provide public online access to a reliable and accurate database with contact information for those who register domain names. In determining the appropriate contact information, the entity administering a party's top-level country domain may consider the laws that the party has in place to protect the privacy of its citizens.

With regard to copyright and related rights, the treaty requires each party to give authors, artists, performers and producers of phonograms the right to authorize or prohibit reproduction of their works, performances or phonograms, in any way or in any form, permanent or temporary (including temporary electronic storage).[14] It also requires each party to give authors, artists, performers and producers of

[14] The parties understand that the right of reproduction, as established in this paragraph and in article 9 of the Berne Convention for the Protection of Literary and Artistic Works (1971), and the exceptions permitted by the Berne Convention and by article 15.5.10a of CAFTA-DR are entirely applicable to the digital environment and, specifically, to works in digital form.

phonograms the right to authorize the publication of their original works, or copies thereof, as well as of their performances and phonograms, through sale or other methods of transferring property.

As regards the technological protection of works, CAFTA incorporates the principles of the Berne Convention and TRIPS. Authors, artists, performers and producers of phonograms may invoke these principles to exercise their rights, as well as to prevent unauthorized acts involving their works, performances and phonograms. The parties are to provide sanctions for: (i) circumventing, without authorization, any effective technological measure controlling access to a protected work, performance or phonogram or other protected object; or (ii) manufacturing, importing, distributing, offering to the public, providing or otherwise trafficking in devices, products or components – or offering to the public or providing services that are publicly promoted, advertised or marketed – for the purpose of circumventing an effective technological measure, or that are designed, produced or executed principally for the purpose of permitting or facilitating circumvention of any such effective technological measure.

Each party is to establish exceptions applying to works, such as permitted activities related to computer programs, that involve:

(i) reverse engineering of legally obtained copies of a program with the sole purpose of making the program interoperable with other programs;
(ii) activities carried out in good faith by a properly qualified researcher who has legally obtained a copy, performance or sample of the work, an unfixed performance, or a phonogram, with the sole purpose of identifying and analysing deficiencies and vulnerabilities of the technology as related to the coding and decoding of information;
(iii) inclusion of a component or part with the sole purpose of preventing online access by minors to inappropriate content;
(iv) permitted activities carried out in good faith that are authorized by the owner of a computer, computer system or computer network, with the sole purpose of testing, investigating or correcting the security of said computer, system or network.

The treaty also protects information related to rights management**,** and authorizes the parties to provide sanctions for knowingly and without authorization causing, permitting, facilitating or covering up a violation of copyright or a related right by:

(i) deleting or altering any rights-management information;
(ii) distributing or importing for distribution rights-management information that has been altered or deleted; or
(iii) distributing, importing for distribution, transmitting, communicating or making available to the public copies of works, performances or phonograms, knowing that the rights-management information has, without authorization, been deleted or altered. Sanctions are to apply if it is demonstrated that the action has not been taken by a library, archive, educational institution or public non-profit broadcaster, and that the perpetrator has fraudulently acted to obtain a commercial advantage or private financial gain through any such activity.

CAFTA-DR also obligates all central government agencies to use only licensed computer programs. Thus, each party must issue the decrees, laws, ordinances or regulations needed to actively regulate the acquisition and management of computer programs so as to comply with this requirement.

Each party must give authors the exclusive right to authorize or prohibit the direct or indirect wired or wireless publication of their works. Publication includes making works available in such a way that members of the public have access to them from whatever place and at whatever time they choose.

With regard to the protection of coded program-carrying satellite signals, CAFTA-DR obligates the parties to prohibit the manufacture, assembly, modification, importation, exportation, sale, rental or other type of distribution of a tangible or intangible device or system with the knowledge, or having reason to know, that said device or system serves primarily to decode a coded program-carrying satellite signal, without the authorization of the legitimate distributor of said signal. Parties are also required to prohibit the reception and subsequent fraudulent distribution of a program-carrying signal that has originated as a coded satellite signal with the knowledge that it has been decoded without the authorization of its legitimate distributor.

Another important aspect of the treaty is its inclusion of limited liability for providers of services involving:

(i) transmission, routing or provision of connections for materials without modifying their content, or intermediate transitory storage of material in the course of the above-mentioned activities;
(ii) temporary storage through an automatic process (caching);
(iii) storage, at the request of the user, of the material housed on a system or network controlled or operated by or for the service provider, and
(iv) referring or providing links for users to a website in the form of search tools, including hyperlinks and directories.

Thus, the treaty establishes the constraints that parties must incorporate in their legislation regarding the range of resources available to take action against the above-mentioned service providers in cases of violations of copyright and/or related rights. The limitations on liability apply only in cases where the service provider has not initiated the material's chain of transmission, has not selected the material, and has expeditiously withdrawn or disabled access to the material upon receiving effective notification of a claim of violation of copyright and/or related rights. The only compensation that can be required of the provider is termination of specific accounts or the adoption of reasonable measures to block access to a specific non-domestic website.

6) Ibero-American Personal Data Protection Network (Red Iberoamericana de Protección de Datos Personales, or RIPD)[15]

The participation of all of the Central American countries in RIPD has encouraged solid interaction between the Spanish Data Protection Agency and the various national agencies involved in protecting personal data. The former entity has been behind the Directives for Harmonization of Data Protection in the Ibero-American Community, which are based on Directive 95/46/CE of the European Parliament and of the Council of the European Union, and encourages members to make relevant legal provisions based on this directive.

B) Current state of cyberlegislation; conclusions

1) Electronic transactions and electronic signature

(i) The region's international commitments

Section 2.1 of the Agenda for Connectivity in the Americas ("Building trust in the digital marketplace"), which deals with e-commerce, states that "Government has a role to ensure that the conditions are in place to permit citizens and businesses to feel secure when they use electronic commerce. Security is a primary area of concern. Governments must establish clear rules permitting the use of cryptography and set policy concerning key recovery. Institutions must also be established to verify and certify electronic signatures in order to validate data messages in law and provide greater security for electronic transactions. E-commerce is encouraged by an environment where the availability of strong encryption and security of communications, data and transactions is assured. Privacy is a second key area where government must play a role."

[15] The network includes: Argentina, the Plurinational State of Bolivia, Brazil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Spain, Guatemala, Honduras, Mexico, Nicaragua, Panama, Paraguay, Peru, Portugal, the Dominican Republic, Uruguay and the Bolivarian Republic of Venezuela. See: https://www.agpd.es/portalweb/internacional/red_iberoamericana/index-ides-idphp.php.

In this connection, the eLAC 2007 Plan aims to facilitate the use of electronic signature in governmental procedures, by public officials and employees as well as citizens, and to promote the adoption of information security and preservation models in all government agencies, so as to generate trust in the digital information managed or provided by the State. It also is intended to encourage the development of electronic contracting mechanisms in government, and to promote the adoption or development of electronic means of payment, so as to encourage the use of electronic transactions with the State and promote the electronic integration of public administration systems through one-stop shops that improve internal governmental procedures and processes.

One of the goals of the eLAC 2010 Plan is to facilitate the use and probative value of electronic documents and electronic/digital signatures in governmental procedures, whether employed by public officials and employees or by citizens. It also attempts to promote the adoption or development of electronic means of payment in order to encourage the use of electronic transactions with the State.

In addition, it aims to strengthen ways of sharing experience in e-government and develop regional cooperation for the exchange and transfer of technologies, platforms, applications and computer programs, along with knowledge, skills and best practices in these areas.

A further goal is to promote the interoperability of e-government systems in Latin America and the Caribbean using common standards, and to continue developing a regional platform for e-government interoperability and standards, in order to provide the option of interconnecting services within a jurisdiction or between different jurisdictions, bearing in mind such recommendations as those of the White Book of e-Government Interoperability for Latin America and the Caribbean.

One of the most ambitious eLAC 2010 goals is to ensure that 80% of local governments interact with citizens and other branches of government via the internet, or to double the current number of local governments doing so. Moreover, the goal is to ensure that 70% of national and local government entities are connected, using a one-stop shop approach for citizens' transactions, or to double the current number, as the case may be.

(ii) International normative instruments

In order to implement a common legislative framework based on uniform legal standards and to supplement the legal regime established by CAFTA-DR, the member countries have worked with the UNCITRAL General Secretariat to adopt treaties and laws based on the UNCITRAL model laws in the areas of arbitration, purchase/sale of goods and e-commerce. In the e-commerce area, Guatemala, Honduras, the Dominican Republic, Panama and the United States have reported significant advances in regard to the adoption of the United Nations Convention on the Use of Electronic Communications in International Contracts (CUECIC). This convention will enter into effect for its signatory countries once three ratifying instruments have been deposited with the United Nations Secretariat.

The Dominican Republic, Guatemala and the United States have also passed legislation based on the UNCITRAL model laws. Costa Rica's law on digital certificates, signatures and documents incorporates the principal provisions of the UNCITRAL Model Law on Electronic Signatures, and legislative bills in El Salvador and Nicaragua have taken account of the Model Law on Electronic Commerce and Electronic Signatures, as well as CUECIC.

Similarly, the regulation of electronic media in RECAUCA, which is the basis for the Central American Commission on Electronic Certification, is an important element for the normative harmonization of the participating countries.

(iii) Regulations in the participating States

A review of the normative provisions of the countries participating in the UNCTAD Regional Workshop on Cyberlegislation in San Salvador revealed two regulatory trends in Central America.

The first of these is the adoption of special laws on electronic signature, some of which also cover issues of electronic contracting and data messages in civil, mercantile, tax and/or administrative contexts. Among the countries adopting such laws are Costa Rica, Guatemala, Panama and the Dominican Republic. In

addition, some of these countries have issued administrative regulations governing the functioning of their digital signature infrastructure. Thus, Costa Rica has operational and coordination-related regulations implementing its Decree 33018, which deals with certificates, digital signatures and electronic documents. Both El Salvador and Nicaragua have followed this trend of special laws in developing their electronic signature bills.

The second trend is exemplified by Honduras, which has amended various civil, mercantile, administrative and tax laws to recognize the use of electronic media and signatures.

Some countries have implemented government procurement systems that employ online transactions. Costa Rica's electronic system, CompraRED, and Guatemala's GUATECOMPRAS system are notable in this respect. Nicaragua and Panama have also changed their administrative regulations to implement online procurement systems for governmental entities.

None of the questionnaires completed by the above-mentioned countries indicated that they had drawn on the 1996 Model Law on Electronic Commerce or the 2001 Model Law on Electronic Signatures in designing their special laws on government contracting.

The Central American Customs Union has modernized its customs procedures, employing a one-stop shop approach for foreign trade operations, among other measures, pursuant to WTO and RECAUCA commitments and commitments to free trade agreements with the United States and Canada. As regards national regulations, the Dominican Republic's provisions authorize electronic payment through its Foreign Trade Single Window.

In the tax area, the use of electronic invoices is allowed under tax laws in El Salvador, Guatemala, Honduras, Panama and the Dominican Republic. In addition, the laws of El Salvador, Guatemala and the Dominican Republic permit taxpayers to file tax statements and pay taxes online.

(iv) Conclusions

Under countries' commitments to the eLAC 2007 and eLAC 2010 Regional Plans, regional goals were established that will influence the development of e-commerce, as well as e-government, through the adoption of mechanisms that use digital signatures and certificates, as well as through the use of the one-stop shop concept, providing compatibility between different government agencies and different States in the region.

In addition to the advances represented by RECAUCA, CAFTA-DR and the United States-Panama Trade Promotion Agreement, three of the seven countries that participated in the UNCTAD workshop have adopted internal regulations in conformity with the UNCITRAL Model Law on Electronic Commerce, three have adopted the Model Law on Electronic Signatures and two have signed the United Nations Convention on Contracts for the International Sale of Goods via electronic media, while another two have made progress towards its adoption.

Panama also incorporated various elements of the European Commission Directives on Electronic Signatures, Electronic Commerce and Distance Selling in its regulations.

In light of the above, it is considered desirable for those States that have not incorporated the UNCITRAL model laws in their legislation to do so, and for States that have not yet signed the Convention to sign it, in order to harmonize legislation among the region's countries and provide a legal foundation for, among other things, international recognition of electronic signatures and digital certificates issued in the region's various countries, as a means of facilitating cross-border trade.

Normative harmonization is also necessary in the areas of civil, mercantile, tax and administrative law at all levels of government, in order to encourage the simplification of administrative procedures and streamline governmental activity. Duplicate procedures lead to unnecessary infrastructure and processing costs, producing governmental inefficiency and lack of transparency.

With regard to digital signature legislation, normative harmonization may encourage cross-recognition of digital certificates issued by different certification entities, both public and private, within countries and between them.

Regional standards also need to be harmonized in conformity with the guidelines set forth in the White Book of e-Government Interoperability for Latin America and the Caribbean – ECLAC, incorporating the standards and recommendations of the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT), as well as UNeDocs and Recommendation 33 on the Single Window.

In another area, it should be noted that CAFTA-DR establishes legislative measures to limit the liability of internet service providers (ISPs) in the context of intellectual property rights in e-commerce, by establishing mechanisms for notification and removal of illicit materials, with a view to encouraging online activities. The United States Digital Millennium Copyright Act has been a significant influence in this respect.

Furthermore, the commitments in the eLAC 2007 and eLAC 2010 Regional Plans call for leadership by a supranational entity such as the Central American Integration System (SICA), in order to encourage countries to incorporate, in their public policies, the normative instruments needed to achieve the plans' goals.

In this connection, it is of paramount importance to define a plan of action with the SICA General Secretariat, in order to support the creation and implementation of a regional framework for e-commerce, and to move towards recognizing and issuing digital documents and signatures. The efforts of the UNCTAD/TrainForTrade working groups and platform should be used as a source for stimulating discussion and further work in this area.

2) Consumer protection

(i) The region's international commitments

In the area of consumer protection, one of the issues that has become increasingly important is the threat of spam. The Tunis Agenda for the Information Society (2005) addressed this matter in the following terms:

"We resolve to deal effectively with the significant and growing problem posed by spam. We take note of current multilateral, multi-stakeholder frameworks for regional and international cooperation on spam, for example, the APEC Anti-Spam Strategy,[16] the London Action Plan, the Seoul-Melbourne Anti–Spam Memorandum of Understanding and the relevant activities of the Organization for Economic Cooperation and Development (OECD) and the International Telecommunications Union (ITU). We call upon all stakeholders to adopt a multi-pronged approach to counter spam that includes, *inter alia*, consumer and business education; appropriate legislation, law-enforcement authorities and tools; the continued development of technical and self-regulatory measures; best practices; and international cooperation."

The eLAC 2007 goals include promoting dialogue, regional exchange and cooperation in regard to national experiences with spam and related institutional and technological issues. The plan also stresses the desirability of creating subregional working groups to develop and promote policies to harmonize legal provisions and standards. The ultimate objective here is to have legislative frameworks that build confidence and security, at both national and regional levels. Special attention should be given to legislation on spam, as part of the framework needed for the development of the information society.

The eLAC 2010 Regional Plan calls for designing and executing policies that foster the healthy development of e-commerce, including education for providers and consumers on their rights and obligations.

[16] Asia-Pacific Economic Cooperation

(ii) International normative instruments

United Nations General Assembly Resolution 39/248, Guidelines for Consumer Protection, approved in 1985, has helped shape legislation in nearly all of the participating countries. It sets forth basic principles governing consumer relationships, and affirms consumers' right to real and effective protection in transactions made through electronic media, as well as their right not to have their personal data used in improper ways.

The OECD Guidelines for Consumer Protection in the Context of Electronic Commerce (1999) also recognize these rights, and the OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders strengthens online consumer protections.

OECD has also issued a Recommendation on Cross-Border Cooperation to promote the effective enforcement of laws combating spam (2006), and a Recommendation on Cross-Border Cooperation in the Enforcement of Laws Protecting Privacy (2007), designed to increase online protections for consumers.

The Asia-Pacific Economic Cooperation (APEC) Privacy Framework, a result of the Data Privacy Pathfinder project, provides a multilingual system that permits the private sector to create its own cross-border rules for the protection of consumer privacy and personal information through seal-of-trust schemes.

(iii) Regulation in the participating States

In incorporating the basic consumer rights set forth in United Nations General Assembly Resolution 39/248 (Guidelines for Consumer Protection), the States have adopted provisions that, among other things, prohibit misleading advertising and abusive clauses in membership contracts.

However, it should be noted that the laws of Costa Rica, El Salvador, Guatemala and Nicaragua make no explicit mention of e-commerce operations. Only Honduras, the Dominican Republic and Panama have explicit provisions in this area. Sections of Honduran and Dominican laws governing sales made outside a provider's place of business establish a minimum regulatory framework. Panamanian law recognizes the use of codes of conduct to promote confidence in e-commerce.

For purposes of self-regulation, various national chambers and associations have developed codes of conduct and seal-of-trust schemes for application in e-commerce. The participation of the countries that are part of CAFTA-DR and of the United States-Panama Trade Promotion Agreement has encouraged the adoption of such mechanisms.

(iv) Conclusions

The creation of a common consumer protection regime through a framework treaty incorporating international best practices such as those endorsed by OECD or APEC can strengthen consumer confidence, especially in regard to cross-border online transactions. In addition, the spread, in Central America, of self-regulatory mechanisms such as seals of trust can increase consumer confidence in e-commerce. Progress on harmonized provisions governing economic competition within the region will also encourage the development of markets in a way beneficial to consumers.

3) Privacy and protection of personal information

(i) The region's international commitments

Section 39 of the Tunis Agenda for the Information Society (2005) emphasizes the need to continue promoting, developing and implementing a global culture of cybersecurity. This requires national action, as well as greater international cooperation, in order to strengthen protections for information, privacy and personal data, as required by United Nations General Assembly Resolution 57/239.

Similarly, the goals of the eLAC 2007 Regional Plan include the creation of subregional working groups to develop and promote policies to harmonize laws, regulations and standards. Here, the objective is to create legislative frameworks that provide confidence and security, both nationally and regionally. Special

attention should be given to legislation protecting privacy and personal information, as part of the framework needed for the sound development of the information society.

The eLAC 2010 goals include linking national health websites in an eventual regional network for sharing experiences and content, and promoting its development, adaptation and relevance, with a view to the proper protection of data.

(ii) International normative instruments

The participating countries have adopted the principles of the Universal Declaration of Human Rights and the Inter-American Convention on Human Rights (San José Pact) regarding the protection of individual privacy provided in national constitutions.

OECD has issued various recommendations on the protection of personal information, including its 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These guidelines have facilitated the harmonization of international normative frameworks and have helped to safeguard the basic right to the protection of personal information in a context of new threats from the online environment – threats such as illicit disclosure of personal information, illegal storage of such data, storage of inaccurate data and improper alteration of data.

The guidelines are voluntary, and are aimed at governments, as well as at private enterprise, other organizations and individual users. They include principles that cover all media involved in the computerized processing of personal information — as well as all possible types of information processing and all types of personal data — and set minimum standards for the effective protection of personal information at the different stages of their acquisition, processing and transmission.

Another multinational organization that has worked on these issues is APEC. Its "Privacy Framework" includes practical measures to protect the privacy of physical persons in a way that achieves a balance between this fundamental right and the business needs of firms. The principles that it sets forth reflect the cultural plurality of the APEC countries. Emphasis is on the reasonable expectations of consumers, and on the requirement that businesses recognize and safeguard consumers' right to privacy.

The Framework's objectives are: (i) to permit multinational organizations that compile, access, use and/or process information in APEC economies to access and use personal information from any participating economy, through the development and implementation of uniform approaches within their organizations; and (ii) to make it possible for the agencies responsible for protecting personal data to fulfill their legal mandate.

The Ibero-American Data Protection Network, of which all of the participating countries are a part, uses the Directives for Harmonization of Data Protection in the Ibero-American Community to regulate: (i) principles governing the purpose and nature of data; (ii) measures to ensure proper handling of data; (iii) information that must be provided to the party concerned; (iv) right of said party to access, correct and remove data; (v) other rights of such parties; (vi) security and confidentiality in processing data; (vii) constraints on international data transfers; (viii) supervisory entities; and (ix) sanctions.

Among the principal measures related to the supervisory entities, the Directives cite: (i) providing these entities their own corporate status if they are not part of a pre-existing governmental entity; (ii) establishing mechanisms to guarantee the independence and tenure of the heads of such entities; (iii) maintaining a record of the data processing carried out by the public and private sectors, and making it available to the parties concerned; (iv) authorizing international transfers of data to States whose legislation does not include the provisions set forth in the Directives; (v) promoting the use of self-regulatory mechanisms; and (vi) creating mechanisms for bilateral and multilateral cooperation with other official entities.

(iii) Regulation in the participating States

Privacy protection has been addressed at the constitutional level by Costa Rica, Guatemala, El Salvador and the Dominican Republic. Honduras, Nicaragua, and Panama have, in addition, recognized the right of habeas data in order to guarantee access to, as well as correction and/or removal of, personal data that jeopardize personal and family privacy.

With regard to national legislation, the participating countries have no general law on data protection that applies to all situations in which personal data are collected, processed and stored – such as the law proposed by the Directives on Data Protection in the Ibero-American Community, which follows the European model set forth in European Council Directive 95/46. Rather, the countries have adopted a variety of sectoral laws on governmental procedures in areas such as taxes, customs, finance and telecommunications.

El Salvador's Banking Law and Electronic Book-Entry Securities Law protect information subject to financial and securities market secrecy. Costa Rica's General Telecommunications Act (Law 8642) protects the inviolability of communications, incorporating various measures taken from the Directives regarding privacy in electronic communications, and prohibiting, among other things, e-mail for direct marketing (spam) without the prior consent of the owner of the e-mail account. The Dominican Republic's General Telecommunications Act (Law 153-98) also protects the inviolability of telecommunications. Nicaragua's Transparency and Access to Public Information Act has certain provisions protecting personal data in the possession of government entities, and includes a habeas data provision.

(iv) Conclusions

The adaptation of national legal provisions to conform to the Directives for Harmonization of Data Protection in the Ibero-American Community facilitates cross-border trade with the European Union. However, it is important to consider measures that provide compatibility with CAFTA-DR, as well as with the United States-Panama Trade Promotion Agreement and the Canada-Costa Rica Free Trade Agreement. Also important is the spread of self-regulatory schemes such as those involving cross-border seals of trust in the APEC Data Privacy Pathfinder project.

4) Cybercrime

(i) The region's international commitments

The eLAC 2007 Regional Plan is designed to promote dialogue, sharing and regional cooperation on national experiences with cybersecurity, spam and related institutional and technological matters. Its goals include creating subregional working groups to promote and develop policies to harmonize laws, regulations and standards, with a view to creating legislative frameworks that provide confidence and security, both nationally and regionally. The plan also draws attention to the need for legislation on cybercrime and crimes employing ICT, as part of the framework necessary to the sound development of the information society.

The plan also emphasizes the need to promote existing regional initiatives that integrate ICT in national systems of justice – for example, projects such as the Electronic Justice Project of the supreme courts of the Ibero-American countries.

The eLAC 2010 Regional Plan invites the countries to study the possibility of ratifying or signing the Council of Europe Convention on Cybercrime and its additional protocol, as a way to facilitate normative integration and adaptation in this field, while observing privacy-protection principles.

(ii) International instruments

The Council of Europe Convention on Cybercrime and its additional protocol address issues of substantive and procedural criminal law. They obligate member States to implement measures incorporating their provisions in national legislation, while also providing for international cooperation.

The Convention covers four substantive categories of crimes. These constitute a minimum list, including the extraditable crimes enumerated below and the elements to be included in defining the crimes.

I. Crimes against the confidentiality, integrity and availability of computer data and systems: (i) illicit access to a computer system; (ii) illicit interception of computer data; (iii) interfering with (damaging, deleting, altering) data; (iv) interfering with a system (introducing, transmitting, damaging, erasing, causing deterioration in, altering or deleting data); (v) use of devices (software or passwords) to commit crimes.

II. Cybercrime: (i) cyberforgery; and (ii) computer fraud.

III. Crimes involving content: (i) crimes involving child pornography; and (ii) crimes of xenophobia.

IV. Crimes involving intellectual property and related rights.

The Convention sets forth the principal measures for enforcing procedural provisions, as well as conditions and safeguards for human rights, procedures for the immediate preservation of stored data, the requirement that service providers furnish information requested by authorities in the course of an investigation, the searching and confiscation of stored data, the procuring of computer data in real time, the interception of content-based data, jurisdictional issues, and international cooperation, including extradition, mutual assistance and the 24/7 Network.

The agendas of the ITU, OECD, APEC and OAS all promote activities to foster online security and training for various administrative, judicial and parliamentary authorities in areas related to cybercrime. Examples of this are the ITU 2007-2009 Cybercrime Programme to Assist Developing Countries; the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (2002); the APEC Judge and Prosecutor Training Programme for Cybercrime (2005-2008); and the work of the Inter-American Telecommunication Commission (CITEL) Rapporteur Group on Cybersecurity and Critical Infrastructure.

CITEL, CICTE (the Inter-American Committee Against Terrorism) and REMJA (the Meeting of Ministers of Justice and Attorneys General of the Americas) have instituted collaborative mechanisms to create a hemisphere-wide cybersecurity strategy, pursuant to OAS General Assembly Resolution AG/RES 2004 (XXXIV-0/04) of 8 June 2004, entitled "Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity". These organizations have also encouraged the adoption of legislation, along the lines of the Council of Europe Convention on Cybercrime, such as the Dominican Republic's Law 53-07**,** the High-Technology Crimes and Misdemeanours Act**.**

(iii) Regulation in the participating States

Of the countries participating in the workshop, only the Dominican Republic has passed a special cybercrime law. Costa Rica, Guatemala, Honduras and Nicaragua have incorporated certain cybercrimes in their penal codes. In addition, Honduras's Anti-Money Laundering Act and Panama's Law 51 provide sanctions for certain types of cybercrime. El Salvador's Anti-Terrorism Act and Special Law to Punish Customs Violations cite a number of crimes involving information systems. However, neither the Penal Code nor the Code of Criminal Procedure mentions this type of crime.

Crimes commonly subject to sanctions include the interception of communications, computer espionage, illicit access to computer systems, causing harm to information technology systems, computer sabotage, fraud by electronic means, forgery of electronic or computerized documents, interrupting of communications, deleting or altering digital evidence**,** unauthorized disclosure or dissemination of data contained in a computer system, child pornography using electronic media, and violation of intellectual property rights on a commercial scale.

Procedurally, the interception of private communications pursuant to judicial mandate is commonly allowed in criminal investigations. Beyond this, however, little progress has been made on the procedural front. In view of the participating countries' signing of the OAS Mutual Legal Assistance Treaty, which provides for implementation of a 24/7 procedural cooperation mechanism, the incorporation of this institution in domestic legislation has the potential to strengthen the legal framework for investigative, ministerial and judicial authorities. The experience of the Dominican Republic represents an important step forward in the region.

(iv) Conclusions

Ratification of the Council of Europe Treaty on Cybercrime and its additional protocol by the participating countries, and the corresponding modification of substantive and procedural criminal law, would be a major step forward for regional harmonization, as well as for cooperation with Canada, United States, Japan, South Africa and the countries of the European Union. The definition of crimes involving spam, as

well as those defined in CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing Act), can provide legal elements that effectively support efforts to combat this harmful practice.

Inviting legislative and judicial authorities to participate in training programmes and in the ITU Global Cybersecurity Agenda is also important.

5) Intellectual property

(i) The region's international commitments

The goals of the eLAC 2007 Regional Plan, designed to foster efficiency and social inclusion, include creating a regional working group to discuss experiences and share criteria for the development and use of open-source software and freeware. Such a group would also study: the technical, economic, organizational, training and security challenges involved; the use of proprietary software to disseminate best practices and maximize efficiency; coexistence with other forms of licensing; interoperability; and possibilities of migration.

The plan also proposes creating a regional working group, with participation by all interested groups, to investigate the development of the creative and content-development industries and the challenges facing them. The group would also be charged with establishing regional cooperation mechanisms and seeking solutions to common problems such as those involved in financing an economy of intangible goods, achieving distribution of the region's cultural and communications goods and services, and increasing local capacity to produce content while respecting cultural diversity and identity.

The eLAC 2010 Plan proposes the creation of a regional digital content and services market through a public-private partnership with commercial providers, and the holding of forums. It also aims to facilitate access to the resources and capacities needed to develop technology firms (hardware, software, content and services) and to stimulate innovation in existing firms, with special priority given to micro, small and medium-sized enterprises.

In addition, the plan aims to create regional networks using international public-private partnerships of various kinds to promote the development of competitive software in international markets, with special consideration of local needs for productive and social organizational processes, and with an emphasis on digital inclusion. A further goal of the plan is to encourage the production of interactive and interoperable digital content based on existing initiatives or on the creation of new instruments, such as national centres of excellence. These should be interoperable in the region, should use high-speed networks, and should generate information that is accessible through various channels (including cell phones, fixed telephony, television, radio, computers and film).

(ii) International instruments

There is greater normative harmonization in the area of intellectual property than in other areas, since all of the countries participating in the workshop have signed CAFTA-DR (and also, in the case of Panama, the Trade Promotion Agreement with the United States), as well as the WTO TRIPS Agreement, the Paris Convention, the Berne Convention, the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT).

(iii) Regulation in the participating States

The countries have provided separate regulations for industrial property rights, on the one hand, and copyright and related rights, on the other.

Industrial property rights regulations generally do not consider computer programs, in isolation, to be patentable inventions. They do protect industrial and/or commercial secrets held in electronic form.

The Honduran Industrial Property Act is notable in that it recognizes the use of a distinguishing sign in a domain name or e-mail address as constituting the use of a trademark. Similarly, the scope of Nicaragua's Law 380, the Trademarks and Other Distinguishing Signs Act, covers cyberpiracy of trademarks in domain names.

With regard to intellectual property rights provisions, the laws largely coincide in the ways in which they protect the authors of computer programs and databases, those holding rights to them, and the holders of copyright-related rights.

The definition of crimes involving the illicit reproduction of materials with counterfeit trademarks on a commercial scale, and of works protected by copyright, has also been included in the legislation of many of the countries participating in the workshop. However, the levels of piracy in the region highlight the problems of providing effective enforcement.

(iv) Conclusions

Although there is a high degree of harmonization in this area, given the signing of various international treaties administered by WIPO and the commitments assumed by countries under CAFTA-DR and the United States-Panama Trade Promotion Treaty, there still need to be changes in domestic laws and regulations in order to comply with these international commitments..

6) Domain names

(i) The region's international commitments

The eLAC 2007 Regional Plan proposes to promote dialogue, interchange and regional cooperation on national experiences on various issues: internet governance, training in internet resources management (domain names, IP numbers and protocols), international connection costs, cybersecurity, spam and related institutional and technological matters.

(ii) International instruments

The coordination of the region's internet registry authorities through the Latin American and Caribbean Internet Addresses Registry (LACNIC), with global coordination by ICANN, is one of the cornerstones of internet development in Central America. In this regard, the adoption of the ICANN Uniform Domain-Name Dispute-Resolution Policy is of paramount importance for regional harmonization of the criteria of registry authorities.

(iii) Regulation in the participating States

With regard to domain names, CAFTA-DR obligates its member countries to create mechanisms to combat cyberpiracy by implementing procedures based on the principles of the ICANN Uniform Domain-
Name Dispute-Resolution Policy. The dispute resolution procedures employed 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 inhibit the development of cross-border business for the region.

(iv) Conclusions

It is essential that the change from IPV4
o IPV6 protocol be promoted in the internet community in all participating countries, through specialized global forums such as the Internet Governance Forum (IGF) and the South School on Internet Governance.

IV. ANNEXES

The foregoing studies of individual countries are supplemented by tables showing the level of regulatory harmonization with international instruments. The legend applicable throughout is as follows.

Legend for tables of regulatory/legislative frameworks

Framework harmonized with international instruments of specialized United Nations organizations

Framework harmonized with international instruments of organizations not pertaining to United Nations organizations

National regulations not harmonized with international instruments

No regulations in force

Green letters	- Legislative bill - Influence of international instruments of specialized United Nations organizations
White letters	- Influence of international instruments of specialized organizations not belonging to the United Nations

Costa Rica

Electronic transactions	Electronic signature and authentication	Consumer protections	Data protection	Cybercrime	Intellectual property	Domain names	Taxes and customs
Law 8454: Certificates, Digital Signatures and Electronic Documents Act UNCITRAL e-signature Law 63: Civil Code Law 3284: Commercial Code Law 7494: Government Contracting Decree 32717: Regulations on Use of Governmental Purchasing System CompraRED Law 8220: Citizen Protection from Excessive Administrative Requirements and Procedures Act Decree 35139: Established Inter-Agency Commission on Digital Government CUECIC	Law 8454: Certificates, Digital Signatures and Electronic Documents Act UNCITRAL e-signature Decree 33018: Regulations for Certificates, Digital Signatures and Electronic Documents Act	Law 7472: Promotion of Competition and Effective Consumer Protection Act UN Resolution 39/248	Costa Rican Constitution San José Pact Law 8642: General Telecommunications Act EU Directive 2002/5846: Privacy and Electronic Communications Law 8634: Insurance Market Regulation Act CAFTA-DR Directives for Harmonization of Data Protection in the Ibero-American Community	Penal Code	WIPO Copyright Treaty; WIPO Performances and Phonograms Treaty Berne Convention (works) Paris Convention Geneva Convention (phonograms) Protocol to the Central American Convention on the Protection of Industrial Property CAFTA-DR Rome Convention TRIPS Agreement Law 6683: Copyright and Related Rights Act Law 6867: Patents, Industrial Designs and Models Act	CAFTA-DR Policy for operation of top-level domain ".cr" ICANN dispute resolution – WIPO Arbitration and Mediation Centre	Law 8454: Certificates, Digital Signatures and Electronic Documents Act UNCITRAL e-signature CAUCA RECAUCA CAFTA-DR Canada Free Trade Agreement Law 7557: General Customs Act Law 8220: Citizen Protection from Excessive Administrative Requirements and Procedures Act

Dominican Republic

Electronic transactions	Electronic signature and authentication	Consumer protections	Data protection	Cybercrime	Intellectual property	Domain names	Taxes and customs
Law 126-02: Electronic Commerce, Documents and Digital Signature Act UNCITRAL e-commerce and e-signature CUECIC Law 184-02: Monetary and Financial Code Law 19-2000 on the Securities Market RECAUCA CAFTA-DR	Law 126-02: Electronic Commerce, Documents and Digital Signature Act UNCITRAL e-commerce and e-signature CUECIC	Law 358-05: General Consumer Protection Act UN Resolution 39/248	Constitution of the Dominican Republic San José Pact Law 153-98: General Telecommunications Act Law 53-07: High-Technology Crimes and Misdemeanours Act Council of Europe Convention on Cybercrime Law 200-04 on Free Access to Public Information Law 288-05, creating credit information bureaus Law 495-06: Tax Rectification Act CAFTA-DR Directives for Harmonization of Data Protection in the Ibero-American Community	Penal Code Law 53-07: High-Technology Crimes and Misdemeanours Council of Europe Convention on Cybercrime	Constitution of the Dominican Republic WIPO Copyright Treaty and Performances and Phonograms Treaty Berne Convention (works) Paris Convention Geneva Convention (phonograms) Protocol to the Central American Convention on the Protection of Industrial Property CAFTA-DR Rome Convention TRIPS Agreement Law 20-00, on industrial property Law 65-00, on copyright	CAFTA-DR Registry policy does not incorporate ICANN UDRP	Law 495-06: Tax Rectification Act Decree 248-09 of 9 July 1998, creating the Integrated Foreign Trade Single Window System (SIVUCEX) CAUCA RECAUCA CAFTA-DR

El Salvador

Electronic transactions	Electronic signature and authentication	Consumer protections	Data protection	Cybercrime	Intellectual property	Domain names	Taxes and customs
Civil Code Commercial Code CAFTA-DR Banking Law Electronic Book-Entry Securities Law Law on uniform procedures for the submission, processing and recording/deposit of instruments in the Real Estate and Mortgages, Social Property, Commercial, and Intellectual Property Registries Digital Signature bill UNCITRAL e-commerce and e-signature CUECIC	Communication and Electronic Signature Act UNCITRAL e-commerce and e-signature CUECIC	Salvadoran Constitution Consumer Protection Act UN Resolution 39/248	Salvadoran Constitution San José Pact Law on Names of Natural Persons Banking Law Electronic Book-Entry Securities Law Customs Simplification Act Data Protection Bill CAFTA-DR Directives for Harmonization of Data Protection in the Ibero-American Community	Anti-Terrorism Act Special Law for Sanctions on Customs Violations	Salvadoran Constitution WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty Berne Convention Paris Convention Geneva Convention (phonograms) Protocol to the Central American Convention on the Protection of Industrial Property CAFTA-DR Rome Convention TRIPS Agreement Intellectual Property Act Trademarks and other Distinguishing Signs Act	CAFTA-DR Trademarks and other Distinguishing Signs Act ICANN Uniform Domain-Name Dispute-Resolution Policy and Regulations AMCHAM Mediation and Arbitration Centre	Tax Code Customs Simplification Act CAUCA RECAUCA CAFTA-DR

Guatemala

Electronic transactions	Electronic signature and authentication	Consumer protections	Data protection	Cybercrime	Intellectual property	Domain names	Taxes and customs
Electronic Communications and Signature Recognition Act UNCITRAL e-commerce and e-signature CUECIC Civil Code Commercial Code Bank of Guatemala Charter Act Securities Market and Merchandise Act State Procurement – GUATECOMPRAS System – Act Digital Signature Bill UNCITRAL e-commerce and e-signature CUECIC RECAUCA CAFTA-DR	Electronic Communications and Signature Recognition Act UNCITRAL e-commerce and e-signature CUECIC	Guatemalan Constitution Consumer and User Protection Act UN Resolution 39/248	Guatemalan Constitution San José Pact Tax Code Banks and Financial Groups Act Public Information Access Act CAFTA-DR Directives for Harmonization of Data Protection in the Ibero-American Community	Penal Code	Guatemalan Constitution WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty Berne Convention (works) Paris Convention Geneva Convention (phonograms) Protocol to the Central American Convention on the Protection of Industrial Property CAFTA-DR Rome Convention TRIPS Agreement Copyright and Related Rights Act Industrial Property Act	CAFTA-DR ICANN Uniform Domain-Name Dispute-Resolution Policy and Regulations (ICANN UDRP) WIPO Arbitration and Mediation Centr	Tax Code CAUCA RECAUCA CAFTA-DR

Honduras

Electronic transactions	Electronic signature and authentication	Consumer protections	Data protection	Cybercrime	Intellectual property	Domain names	Taxes and customs
Commercial Code Financial System Act Securities Market Act State Contracting Act Property Act CUECIC RECAUCA CAFTA-DR	Infotechnology and Electronic Government Framework Law	Honduran Constitution Consumer Protection Act UN Resolution 39/248	Honduran Constitution San José Pact Transparency and Public Information Access Act CAFTA-DR Directives for Harmonization of Data Protection in the Ibero-American Community	Penal Code Assets Laundering Crimes Act	Honduran Constitution WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty Berne Convention (works) Paris Convention Geneva Convention (phonograms) Protocol to the Central American Convention on the Protection of Industrial Property CAFTA-DR Rome Convention TRIPS Agreement Copyright and Related Rights Act Industrial Property Act	CAFTA-DR ICANN Uniform Domain-Name Dispute-Resolution Policy and Regulations (ICANN UDRP) WIPO Arbitration and Mediation Centre	Tax Code General Customs Act CAUCA RECAUCA CAFTA-DR

Nicaragua

Electronic transactions	Electronic signature and authentication	Consumer protections	Data protection	Cybercrime	Intellectual property	Domain names	Taxes and customs
General Banks, Non-Bank Financial Institutions and Financial Groups Act Capital Markets Act State Contracting Act RECAUCA CAFTA-DR	Draft Electronic Signature Act UNCITRAL e-commerce and e-signature CUECIC	Law 182: Consumer Protection Act UN Resolution 39/248	Nicaraguan Constitution San José Pact Public Information Access Act CAFTA-DR Directives for Harmonization of Data Protection in the Ibero-American Community	Law 641: Penal Code	Nicaraguan Constitution WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty Berne Convention (works) Paris Convention Geneva Convention (phonograms) Protocol to the Central American Convention on the Protection of Industrial Property CAFTA-DR Rome Convention TRIPS Agreement Law 380: Trademarks and Other Distinguishing Signs Act Copyright and Related Rights Act Law 354: Patents on Inventions, Utility Models and Industrial Designs Act	CAFTA-DR Law 380: Trademarks and Other Distinguishing Signs Act ICANN Uniform Domain-Name Dispute-Resolution Policy and Regulations (ICANN UDRP) WIPO Arbitration and Mediation Centre	Tax Code CAUCA RECAUCA CAFTA-DR

Panama

Electronic transactions	Electronic signature and authentication	Consumer protections	Data protection	Cybercrime	Intellectual property	Domain names	Taxes and customs
Law 51 of 22 July 2008, defining and regulating electronic documents and electronic signatures and the provision of technological document storage services and electronic signature certification services, and adopting other provisions for e-commerce UNCITRAL e-commerce and e-signature CUECIC European Directives on Electronic Commerce, Electronic Signatures and Distance Selling Commercial Code Civil Code RECAUCA Canada Free Trade Agreement Trade Promotion Treaty with United States CAFTA-DR	Law 51 of 22 July 2008, defining and regulating electronic documents and electronic signatures and the provision of technological document storage services and electronic signature certification services, and adopting other provisions for e-commerce UNCITRAL e-commerce and e-signature CUECIC European Directives on Electronic Commerce, Electronic Signatures and Remote Distance Selling	Panamanian Constitution Law 51 Law 45 UN Resolution 39/248	Panamanian Constitution San José Pact Law 51 Executive Decree 52-2008: Adoption of the Consolidated Text of Decree Law 9 of 26 February 1998, amended by Decree Law 2 of 22 February 2008. CAFTA-DR Canada Free Trade Agreement Trade Promotion Treaty with United States Directives for Harmonization of Data Protection in the Ibero-American Community	Law 14: Penal Code Law 51	Panamanian Constitution WIPO Copyright Treaty and WIPO Performances and Phonograms Treaty Berne Convention (works) Paris Convention Geneva Convention (phonograms) Protocol to Central American Convention on the Protection of Industrial Property CAFTA-DR Rome Convention TRIPS Agreement Law 35: Industrial Property Act Law 15 of 8 August 1994, approving the Copyright and Related Rights Act	CAFTA-DR Uniform Domain-Name Dispute-Resolution Policy and Regulations (ICANN UDRP) WIPO Arbitration and Mediation Centre	Decree Law 1 of 13 February 2008, creating the National Customs Authority Law 51 CAUCA RECAUCA CAFTA-DR Canada Free Trade Agreement Trade Promotion Treaty with United State

State of legislation/regulations in the region's countries

The following normative table, based on information from "II—Normative Report of Participating Countries", was created to show the principal advances in normative harmonization in the area of electronic transactions, electronic signature and authentication under RECAUCA and CAFTA-DR, which have favoured incorporation of the UNCITRAL e-commerce and electronic signature model laws. In the area of intellectual property rights, the adoption of CAFTA-DR has brought all of the signatories of that agreement into line with the main WIPO treaties. The table shows lesser advances in normative harmonization in the areas of consumer protection, protection of personal information, cybercrime, domain names, taxes and customs.

Table of regulatory frameworks of Central American countries

Pais	Electronic transactions	Electronic signature and authentication	Consumer protections	Data protection	Cybercrime	Intellectual property	Domain names	Taxes and customs
Costa Rica								
Dominican Republic								
El Salvador								
Guatemala								
Honduras								
Nicaragua								
Panama								

V. BIBLIOGRAPHY

ECLAC (Economic Commission for Latin America and the Caribbean) (2007), *Plan of Action for the Information Society in Latin America and the Caribbean, eLAC 2007* [online] http://www.cepal.org/socinfo/noticias/documentosdetrabajo/5/21685/eLAC%202007%20English.pdf.

Iriarte Ahon, Erick (2008), "Meta 25 eLAC 2007: regulación en la sociedad de la información en América Latina y el Caribe. Propuestas normativas sobre privacidad y protección de datos y delitos información y por medios electrónicos", Santiago, Chile, unpublished.

_____ (2005), "Estado situacional y perspectivas del derecho informático en América Latina y el Caribe", *Project documents*, No. 25 (LC/W.25), Santiago, Chile, Economic Commission for Latin America and the Caribbean (ECLAC).

UNCTAD (United Nations Conference on Trade and Development) (2010), *Study on prospects for harmonizing cyber-legislation in Latin-America*, Geneva.

Costa Rica:

1. Tratado de Libre de Comercio entre Centroamérica, República Dominicana y Estados Unidos. Ley No. 8622, Capítulo 14. http://www.comex.go.cr/acuerdos/cafta/Contenido/CAFTA/textofoliado/14.Comercio%20Electr%C3%B3nico/capitulo14.pdf y http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=3396&nValor3=74701&strTipM=TC
2. Ley de Certificados, Firmas Digitales y Documentos Electrónicos, Ley No. 8454. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=55666&nValor3=60993&strTipM=TC
3. Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos. Decreto Ejecutivo No. 33018. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=56884&nValor3=74725&strTipM=TC
4. Proyecto de Ley de Comercio Electrónico. http://www.asamblea.go.cr/proyecto/16000/16081.doc
5. Ley de Contratación Administrativa, Ley No. 7494. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=24284&nValor3=75407&strTipM=TC
6. Reglamento a la Ley de Contratación Administrativa, Decreto Ejecutivo 33411. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=58314&nValor3=75124&strTipM=TC
7. Reglamento para la Utilización del Sistema de Compras Gubernamentales CompraRED, Decreto Ejecutivo No. 32717. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=55729&nValor3=61056&strTipM=TC
8. Constitución Política de la República de Costa Rica. http://www.pgr.go.cr/scij/busqueda/normativa/normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=871&nValor3=74424&strTipM=TC
9. Ley General de Telecomunicaciones, No. 8642. http://www.pgr.go.cr/Scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=63431&nValor3=72874&strTipM=TC
10. Reglamento sobre Medidas de Protección de la Privacidad de las Comunicaciones. http://www.minaet.go.cr/acerca/viceministro/document_index.html
11. Adición de los artículos 196 Bis, 217 Bis y 229 Bis al Código Penal, Ley No. 4573 para reprimir y sancionar los delitos informáticos. http://www.pgr.go.cr/scij/busqueda/normativa/normas/nrm_repartidor.asp?param1=NRM&param2=1&nValor1=1&nValor2=47430&nValor3=50318&strTipM=FN&lResultado=1&strSelect=sel

12. Ley General de Aduanas, No. 7557. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRM&nValor1=1&nValor2=25886&nValor3=27386&strTipM=FN
13. Adición de nuevos artículos al Código Penal, Ley No. 4573. Expediente No. 16546. http://www.asamblea.go.cr/proyecto/16500/16546.doc
14. Aprobación del Protocolo al Convenio Centroamericano para la Protección de la Propiedad Industrial (marcas, nombres comerciales y expresiones o señales de propaganda), No. 7982. http://www.pgr.go.cr/scij/busqueda/normativa/normas/nrm_repartidor.asp?param1=NRM&param2=1&nValor1=1&nValor2=30458&nValor3=32155&strTipM=FN&lResultado=1&strLib=lib
15. Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual Relacionados con el Comercio, No. 7475. http://www.pgr.go.cr/scij/busqueda/normativa/normas/nrm_repartidor.asp?param1=NRM&param2=2&nValor1=1&nValor2=48111&nValor3=51200&strTipM=FN&lResultado=16&strSelect=sel
16. Arreglo de Lisboa relativo a la protección de las denominaciones de origen y su registro internacional, No. 7634. http://www.pgr.go.cr/scij/busqueda/normativa/normas/nrm_repartidor.asp?param1=NRM&param2=1&nValor1=1&nValor2=27688&nValor3=29289&strTipM=FN&lResultado=3&strLib=lib
17. Convención de Roma sobre la protección de los artistas e intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión, No. 4727. http://www.pgr.go.cr/scij/busqueda/normativa/normas/nrm_repartidor.asp?param1=NRM&param2=6&nValor1=1&nValor2=6415&nValor3=6830&strTipM=FN&lResultado=54&strLib=lib
18. Convenio para proteger de la reproducción no autorizada de fonogramas, No. 6486. http://www.pgr.go.cr/scij/busqueda/normativa/normas/nrm_repartidor.asp?param1=NRM&param2=5&nValor1=1&nValor2=6931&nValor3=7405&strTipM=FN&lResultado=47&strLib=lib
19. Convenio que establece la OMPI, No. 6468. http://www.pgr.go.cr/scij/busqueda/normativa/normas/nrm_repartidor.asp?param1=NRM&param2=6&nValor1=1&nValor2=5379&nValor3=5703&strTipM=FN&lResultado=57&strLib=lib
20. Convenio de Berna para la protección de las obras literarias y artísticas, No. 6083. http://www.pgr.go.cr/scij/busqueda/normativa/normas/nrm_repartidor.asp?param1=NRM&param2=6&nValor1=1&nValor2=9275&nValor3=9942&strTipM=FN&lResultado=59&strLib=lib
21. Convenio para la Protección de la Propiedad Industrial, No. 7484. http://www.pgr.go.cr/scij/busqueda/normativa/normas/nrm_repartidor.asp?param1=NRM&param2=5&nValor1=1&nValor2=22945&nValor3=24309&strTipM=FN&lResultado=43&strLib=lib
22. Convenio sobre la distribución de señales portadoras de programa transmitidos por satélite, No. 2829. http://www.pgr.go.cr/scij/busqueda/normativa/normas/nrm_repartidor.asp?param1=NRM&param2=4&nValor1=1&nValor2=44177&nValor3=46543&strTipM=FN&lResultado=32&strLib=lib
23. Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas (WPPT), No. 7967. http://www.pgr.go.cr/Scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=30975&nValor3=32702&strTipM=TC
24. Tratado de la OMPI sobre Derechos de Autor (WCT), No. 7968. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=45073&nValor3=47525&strTipM=TC
25. Ley sobre Derechos y Derechos Conexos, No. 6683. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=3396&nValor3=74701&strTipM=TC
26. Patentes, Invención, Dibujos y Modelos Industriales y Modelos de Utilidad, No. 6867. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=8148&nValor3=74713&strTipM=TC
27. Protección a Sistemas de Trazados de Circuitos Integrados, No. 7961. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=42205&nValor3=44487&strTipM=TC
28. Ley de Información No Divulgada, No. 7975. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=41810&nValor3=74709&strTipM=TC
29. Ley de Marcas y Otros Signos Distintivos, No. 7978. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=45096&nValor3=72368&strTipM=TC
30. Ley de Procedimientos de Observancia de Derechos de Propiedad Intelectual, No. 8039. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=44448&nValor3=74708&strTipM=TC

31. Reglamento de la Ley de Patentes, Invención, Dibujos y Modelos Industriales y Modelos de Utilidad, No. 15222-MIEM-J. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=14745&nValor3=74017&strTipM=TC
32. Reglamento a la Ley de Derechos de Autor y Derechos Conexos, No. 24611-J. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=24652&nValor3=74822&strTipM=TC
33. Ley que ordena que todo el Gobierno Central se proponga diligentemente prevenir y combatir el uso ilegal de programas de cómputo, con el fin de cumplir con las disposiciones sobre derecho de autor que establece la Ley No. 6683 y sus reformas. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=47957&nValor3=50972&strTipM=TC
34. Reglamento de la Ley de Marcas y Signos Distintivos, No. 30233-J. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=48168&nValor3=74019&strTipM=TC
35. Reglamento de la Ley de Protección a los Sistemas de Trazados de los Circuitos Integrados, No. 32558. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=55357&nValor3=60649&strTipM=TC
36. Reglamento a la Ley de Información No Divulgada, No. 34927-J-COMEX-S-MAG. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=64524&nValor3=74917&strTipM=TC
37. Políticas para el funcionamiento del dominio de nivel superior .CR. www.nic.cr y http://historico.gaceta.go.cr/pub/2008/02/12/COMP_12_02_2008.html
38. Ley de protección de la niñez y la adolescencia frente al contenido nocivo de Internet y otros medios electrónicos, No. 17164. http://www.asamblea.go.cr/proyecto/17100/17164.doc
39. Ley del Sistema Nacional de Bibliotecas (propone una reforma a la Ley de Derechos de Autor), No. 16921. http://www.asamblea.go.cr/proyecto/16900/16921.doc
40. Aprobación del Protocolo por el que se enmienda el Acuerdo sobre los ADPIC, No. 16947. http://www.asamblea.go.cr/proyecto/16900/16947.doc
41. Ley para impulsar el uso de la ciencia, la tecnología y la innovación, Ley No. 16818. http://www.asamblea.go.cr/proyecto/16800/16818.doc
42. Reformas a varios artículos de la Ley de Patentes de Invención, Dibujos y Modelos Industriales y Modelos de Utilidad No. 6867, Ley No. 16141. http://www.asamblea.go.cr/proyecto/16100/16141.doc
43. Reforma de la Ley de Procedimientos de Observancia de los Derechos de Propiedad Intelectual, No. 8039, Ley No. 16453. http://www.asamblea.go.cr/proyecto/16400/16453.doc
44. Reformas a la Ley de Información No Divulgada, No. 7975. http://www.asamblea.go.cr/proyecto/16400/16439.doc
45. Ley sobre resolución alterna de conflictos y promoción de la paz social (Ley RAC), No. 7727. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=26393&nValor3=27926&strTipM=TC
46. Convención sobre el reconocimiento y ejecución de las sentencias arbitrales extranjeras, No. 6157. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=7445&nValor3=7981&strTipM=TC
47. Convención Interamericana sobre Arbitraje Comercial Internacional, No. 6165. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=16178&nValor3=17319&strTipM=TC
48. Mecanismo de solución de controversias comerciales entre Centroamérica. http://www.comex.go.cr/acuerdos/centroamerica/Documents/solucion%20controversias.pdf
49. Reglamento al Capítulo IV de la Ley sobre Resolución Alterna de Conflictos y Promoción de la Paz Social, Decreto Ejecutivo No. 32152. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=54128&nValor3=59213&strTipM=TC
50. Código de Ética del Centro de Resolución Alterna de Conflictos de Consumo. Programa Casas de Justicia de la dirección de apoyo al consumidor. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=55868&nValor3=61217&strTipM=TC
51. Manual de procedimiento del Centro de Resolución Alterna de Conflictos de Consumo. Programa de Casas de Justicia de la Dirección de Apoyo al Consumidor, Decreto Ejecutivo No. 32742. http://www.consumo.go.cr/consumidor/dac/leyes/32742.pdf

52. Manual de funcionamiento del Centro de Resolución Alterna de Conflictos de Consumo. Programa de Casas de Justicia de la Dirección de Apoyo al Consumidor, Decreto Ejecutivo No. 32743. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=55876&nValor3=61223&strTipM=TC
53. Ley de Protección de la Competencia y la Defensa Efectiva del Consumidor, No. 7472. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=26481&nValor3=73511&param2=1&strTipM=TC&lResultado=2&strSim=simp
54. Ley Reguladora del Mercado de Seguros, No. 8635. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=63749&nValor3=73486&strTipM=TC
55. Reglamento a la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, Decreto Ejecutivo No. 25234. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRTC&nValor1=1&nValor2=40187&nValor3=42355&strTipM=TC
56. Reglamento de Tarjetas de Crédito, Decreto Ejecutivo No. 28712. http://www.pgr.go.cr/scij/Busqueda/Normativa/Normas/nrm_repartidor.asp?param1=NRM&nValor1=1&nValor2=44802&nValor3=47246&strTipM=FN

El Salvador:

1. Ley de Simplificación Aduanera. http://www.aduana.gob.sv/publicaciones/2005/catalogo_leyes/Ley_de_Simplificacion_Aduanera.pdf
2. Reglamento para la aplicación del Código Tributario. Disposición Administrativa DACG No. 009-2005 sobre la nueva versión de SIDUNEA 1.18. http://www.csj.gob.sv/leyes.nsf/ef438004d40bd5dd862564520073ab15/793d7c9e80c7735406256b4c005ea723?OpenDocument y http://www.aduana.gob.sv/index.php?option=com_content&task=view&id=218&Itemid=31
3. Convenio de cooperación entre la Dirección General de Aduanas de la República de El Salvador y la Asociación Alianza Empresarial para el Comercio Seguro BASC. http://74.125.113.132/search?q=cache:1pNLwaTw09gJ:www.aduana.gob.sv/publicaciones/pub/2009/Convenio%2520DGA%2520BASC.pdf+estandares+site:aduana.gob.sv&hl=es&ct=clnk&cd=1&gl=sv&client=firefox-a
4. Proyecto de ley de comunicación y firma electrónica y Proyecto de ley de comercio electrónico. www.epais.gob.sv
5. Código Civil. http://www.csj.gob.sv/leyes.nsf/ed400a03431a688906256a84005aec75/d021a93531456bea06256d02005a3af5?OpenDocument
6. Código de Comercio. http://www.csj.gob.sv/leyes.nsf/ed400a03431a688906256a84005aec75/ff12a77cd3a8ce6206256d02005a3df1?OpenDocument
7. Ley de Procedimientos Civiles. http://www.csj.gob.sv/leyes.nsf/ef438004d40bd5dd862564520073ab15/f59b09a27a90d8e106256d02005a3ffb?OpenDocument
8. Ley de Procedimientos Mercantiles. http://www.csj.gob.sv/leyes.nsf/ef438004d40bd5dd862564520073ab15/52def0f78b16688a002564210040f391?OpenDocument
9. Proyecto de Código Procesal Civil y Comercial. http://www.jurisprudencia.gob.sv/pdf/CodProcCivMer.pdf
10. Ley de Protección al Consumidor. http://www.csj.gob.sv/leyes.nsf/ef438004d40bd5dd862564520073ab15/558939c352bcfd140625709800729fa2?OpenDocument
11. Reglamento de la Ley de Protección al Consumidor. http://www.defensoria.gob.sv/descargas/reglamento_ley_protec_c..pdf
12. Anteproyecto de Ley de Protección de Datos. www.epais.gob.sv
13. Amparo 118-2002. Inconstitucionalidad 36-2004. www.jurisprudencia.gob.sv
14. Ley Especial contra Actos de Terrorismo. http://www.csj.gob.sv/leyes.nsf/c8884f2b1645f48b86256d48007011d2/f50b147ff5914eda0625721f00744c15?OpenDocument

15. Ley Especial para Sancionar Infracciones Aduaneras. http://www.csj.gob.sv/leyes.nsf/ef438004d40bd5dd862564520073ab15/d0f9511850e9ba6306256d02005a3d63?OpenDocument
16. Código Penal. http://www.csj.gob.sv/leyes.nsf/ed400a03431a688906256a84005aec75/29961fcd8682863406256d02005a3cd4?OpenDocument
17. Propuesta de reforma al Código Penal para la introducción del delito informático. www.epais.gob.sv
18. Ley de Propiedad Intelectual. http://www.minec.gob.sv/default.asp?id=5&mnu=5
19. Ley de Marcas y Otros Signos Distintivos. http://www.csj.gob.sv/leyes.nsf/ed400a03431a688906256a84005aec75/365999c9b09dbd1e06256c0500573759?OpenDocument
20. Tratado de la OMPI sobre Derecho de Autor (WCT-1996). http://www.aduana.gob.sv/publicaciones/2005/catalogo_leyes/Tratado%20de%20la%20Organizacion%20Mundial%20de%20la%20Propiedad%20Intelectual%20-OMPI-%20sobre%20el%20Derecho%20de%20Autor%20-WCT-%201996.pdf
21. Tratado de la OMPI sobre Interpretación, Ejecución y Fonogramas (WPPT-1996). http://www.csj.gob.sv/Convenios.nsf/ef438004d40bd5dd862564520073ab15/65a5a5b756e9e75d06256824005ec786?OpenDocument
22. Reglamento a la Ley de Fomento y Protección de la Propiedad Intelectual. http://www.csj.gob.sv/leyes.nsf/d99c058e0c4c391306256a8400738426/5942a053a5e921870625644f0067fb88?OpenDocument
23. Ley de Medicación, Conciliación y Arbitraje. http://www.csj.gob.sv/leyes.nsf/ed400a03431a688906256a84005aec75/20b7c715f9759eb506256c320071f78b?OpenDocument
24. Reglamento de la Ley General de Mediación, Conciliación y Arbitraje. http://www.csj.gob.sv/leyes.nsf/d99c058e0c4c391306256a8400738426/b05297e35c5125d206256dbf0058aadb?OpenDocument&Highlight=0,arbitraje
25. Política de Resolución de Controversias de Nombres de Dominio. www.svnet.org.sv
26. Ley de Telecomunicaciones. http://www.siget.gob.sv/documentos/telecomunicaciones/legislacion/ley_de_telecomunicaciones_al_13dic061028.pdf
27. Reglamento de la Ley de Telecomunicaciones. http://www.siget.gob.sv/documentos/telecomunicaciones/legislacion/reglamento_de_la_ley_de_telecomunicaciones0.pdf

Guatemala:

1. Congreso de la República de Guatemala. www.congreso.gob.gt
2. Decreto 57-2008 del Congreso de la República de Guatemala-Ley de Acceso a la Información Pública. http://www.congreso.gob.gt/archivos/decretos/2008/gtdcx57-0008.pdf
3. Decreto No. 47-2008 del Congreso de la República de Guatemala-Ley para el reconocimiento de las comunicaciones y firmas electrónicas. http://www.congreso.gob.gt/archivos/decretos/2008/gtdcx47-2008.pdf
4. Decreto No. 6-2003 del Congreso de la República de Guatemala-Ley de Protección al Consumidor y Usuarios. http://www.congreso.gob.gt/archivos/decretos/2003/gtdcx06-2003.pdf
5. Ley de Derecho de Autor y Derechos Conexos. http://www.rpi.gob.gt/descargas/Ley%20DERECHO%20DE%AUTOR%2033-98.pdf
6. Ley de la Propiedad Industrial. http://www.rpi.gob.gt/descargas/Ley%20Propiedad%20Industrial.pdf
7. Código de Comercio. http://www.infopyme.com/Docs/GT/Offline/Registro/codigodecomercioguatemala.html#Toc156640835.
8. Decreto No. 27-2009, Reformas al Decreto No. 57-92 del Congreso de la República, Ley de Contrataciones del Estado. http://www.guatecompras.gt/servicios/files/DECRETO%20NUMERO%2027-2009.pdf.
9. Decreto No. 57-2008, Ley de Acceso a la Información Pública. http://www.mintrabajo.gob.gt/org/leyes-y-convenios/leyes-ordinarias/Ley-AIP-Decreto-57-2008.pdf/view.

Honduras:

1. Código Civil. http://www.congreso.gob.hn/Códigos/DECRETO%20CODIGO%20CIVIL.pdf.
2. Código de Comercio. http://www.congreso.gob.hn/Códigos/DECRETO%2073%20CODIGO%20COMERCIO.pdf.
3. Ley de Protección al Consumidor. http://www.sic.gob.hn/produccion/documentos/leyes_regalentos/ley_proteccion_al_consumidor2008.pdf.
4. Ley de Propiedad. http://www.ip.hn/descargas/Ley%20de%20la%20propiedad.pdf.
5. Ley de la Propiedad Industrial. http://www.sice.oas.org/int_prop/nat_leg/honduras/lprinda.asp#tit1cu.
6. Ley de Tarjetas de Crédito. http://ftp.cnbs.gov.hn/leyes/Ley_Tarjetas_Credito.pdf.
7. Ley del Sistema Financiero. http://ftp.cnbs.gov.hn/leyes/Ley_Sistema_Financiero.pdf
8. Circular CNBS No.119/2005. Resolución No. 1301/22-11-2005.- Normas para Regular la Administración de las Tecnologías de Información y Comunicaciones en las Instituciones del Sistema Financiero. http://ftp.cnbs.gov.hn/leyes/normativa_seguridad.pdf
9. Ley de Transparencia y acceso a la información pública. http://www.honducompras.gob.hn/Info/LeyTransparencia.aspx
10. Reglamento de la Ley de Transparencia y acceso a la información pública. www.ihnfa.hn
11. Código Penal. Centro de Estudios de Justicia de las Américas. http://www.cejamericas.org/doc/legislacion/codigos/pen_honduras.pdf
12. Ley contra el Delito de Lavado de Activos. http://ftp.cnbs.gov.hn/leyes/leylavado.pdf
13. Ley de Transparencia y Acceso a la Información Pública. http://www.iaip.gob.hn/pdf/Ley_de_Transparencia_2.pdf.

14. Convenio para la protección de los productos de fonogramas contra la reproducción no autorizada de los mismos. http://www.dpi.bioetica.org/legisdpi/wo023es.htm
15. Convención de Roma sobre protección a los artistas, intérpretes o ejecutantes, productores de fonogramas y organismos de radiodifusión. http://www.dpi.bioetica.org/legisdpi/wo001es.htm
16. Convenio de Berna para la protección de obras literarias y artísticas. http://www.dpi.bioetica.org/legisdpi/wo001es.htm
17. Convenio de París para la protección de la propiedad industrial. http://www.dpi.bioetica.org/legisdpi/wo001es.htm
18. Ley de Conciliación y Arbitraje y Reglamento del Centro de Conciliación y Arbitraje de la Cámara de Comercio e Industria de Tegucigalpa. www.ccit.hn/cca/php
19. Tratado internacional UNCITRAL sobre reconocimiento y ejecución de sentencias arbitrales internacionales. www.uncitral.org
20. Ley de Protección al Consumidor. www.sic.gob.hn

Nicaragua:

1. Código Tributario. http://www.dgi.gob.ni/documentos/Codigo%20Tributario%20con%20Reformas%2C%20Leyes%20Nos.%20562%20y%20598.pdf.
2. Ley de Contrataciones del Estado. http://www.asamblea.gob.ni/index.php?option=com_wrapper&Itemid=153
3. Código Aduanero Uniforme Centroamericano (CAUCA). http://legislacion.asamblea.gob.ni/Normaweb.nsf/($All)/4C52EC18CD2BB95606257274005BBF58?OpenDocument
4. Código Penal de la República de Nicaragua. http://www.poderjudicial.gob.ni/arc-pdf/CP_641.pdf
5. Ley de Acceso a la Información Pública. http://www.mitrab.gob.ni/oaip.html.
6. Ley de Mercado de Capitales. http://www.bcn.gob.ni/banco/legislacion/LEYMERCADOCAPITALES.pdf
7. Ley de Derecho de Autor y de los Derechos Conexos. http://www.nicautor.org/index.php?option=com_content&view=article&id=17%3Aarticulos-reformados-de-la-ley-no-312-ley-de-derecho-de-autor-y-derechos-conexos&catid=20%3Aleyes-leyes-nacionales&Itemid=9
8. Situación actual del derecho de autor en Nicaragua. OMPI. www.wipo.int/edocs/mdocs/lac/es/ompi_jpi_bue_06/ompi_jpi_bue_06_1_ni.doc.

9. Ley de Defensa al Consumidor. http://www.mific.gob.ni/docushare/dsweb/Services/Document-292.
10. Reglamento a la Ley 182, Ley de Defensa de los Consumidores. http://www.mific.gob.ni.
11. Política uniforme de solución de controversias en materia de nombres de dominio del NIC NI. http://www.nic.ni/index.php?s=2
12. Ley 354-Ley de Patentes de Invención, Modelos de Utilidad y Diseños Industriales. http://www.sieca.org.gt/publico/ProyectosDeCooperacion/Proalca/PI/354.htm
13. Reformas al Código Penal en materia de delitos en materia de propiedad intelectual. http://www.nicautor.org/index.php?option=com_content&view=article&id=16%3Acodigo-penal-de-nicaragua-ley-no-641-capitulo-x&catid=20%3Aleyes-leyes-nacionales&Itemid=9

Panamá:

1. Ley No 51 de 22 de julio de 2008 que define y regula los documentos electrónicos y las firmas electrónicas y la prestación de servicios de almacenamiento tecnológico de documentos y de certificación de firmas electrónicas y adopta otras disposiciones para el desarrollo del comercio electrónico. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/2000/2008/2008_560_0378.PDF
2. Ley No. 14 de 18 de mayo de 2007, Código Penal. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/2000/2007/2007_553_1705.PDF
3. Ley No. 24 del 22 de mayo de 2002. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/2000/2002/2002_522_0698.PDF
4. Ley No. 14 de 18 de mayo de 2006. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/2000/2006/2006_547_1508.PDF
5. Ley No. 3 de 5 de enero de 2000. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/2000/2000/2000_200_0140.PDF
6. Ley No. 35 de 10 de mayo de 1996. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/1990/1996/1996_139_1461.PDF
7. Ley No. 1 de 5 de enero de 2004 que modifica y adiciona disposiciones a los Códigos Penal y Judicial y a la Ley No. 35 de 1996 y deroga un artículo del Código Penal y de la Ley No. 15 de 1994 referentes a los derechos de propiedad industrial. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/2000/2004/2004_532_1458.PDF
8. Ley No. 15 de 8 de agosto de 1994 por la cual se aprueba la Ley sobre el Derecho de Autor y Derechos Conexos y se dictan otras disposiciones. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/1990/1994/1994_101_1583.PDF
9. Ley No. 41 de 13 de julio de 1995. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/1990/1995/1995_112_1120.PDF
10. Ley No. 3 de 3 de enero de 1996. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/1990/1996/1996_138_0197.PDF
11. Ley No. 5 de 9 de noviembre de 1982. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/1980/1982/1982_018_0068.PDF
12. Ley No. 35 de 31 de enero de 1962. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/1960/1962/1962_038_2006.PDF
13. Ley No. 12 de 3 de mayo de 1999. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/1990/1999/1999_177_0545.PDF
14. Ley No. 3 de 9 de noviembre de 1982. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/1980/1982/1982_018_0125.PDF
15. Ley No. 8 de 24 de octubre de 1974. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/1970/1974/1974_026_0390.PDF
16. Ley No. 93 de 15 de diciembre de 1998. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/1990/1998/1998_167_1626.PDF
17. Ley No. 93 de 15 de diciembre de 1998. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/1990/1998/1998_167_1626.PDF
18. Ley No. 64 de 28 de diciembre de 1934. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/1930/1934/1934_092_0675.PDF
19. Decreto Ejecutivo No. 7 del 17 de febrero de 1998. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/1990/1998/1998_157_1729.PDF

20. Ley No. 44 del 13 de marzo de 1913. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/1910/1913/1913_109_1748.PDF
21. Ley No. 5 del 25 de octubre de 1983. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/1980/1983/1983_017_0664.PDF
22. Ley No. 11 del 23 de octubre de 1975. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/1970/1975/1975_024_2231.PDF
23. Constitución Política de la República de Panamá. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_GACETAS/2000/2004/25176_2004.PDF
24. Ley No. 45 del 31 de octubre de 2007 que dicta normas sobre protección al consumidor y defensa de la competencia y otra disposición. http://www.autoridaddelconsumidor.gob.pa/pdf/default.asp?pagina=Ley45_autoridaddelconsumidor_31octubre2007.pdf
25. Decreto Ejecutivo No. 31 del 3 de septiembre de 1998, por el cual se reglamenta el Título I (monopolios) y otras disposiciones de la Ley No. 29 del 1 de febrero de 1996. http://www.asamblea.gob.pa/APPS/LEGISPAN/PDF_NORMAS/1990/1998/1998_166_1072.PDF

República Dominicana:

1. Tratado de Libre Comercio República Dominicana, Centroamérica, Estados Unidos (DR-CAFTA). http://www.seic.gov.do/comercioexterior/DR_Cafta/menu.aspx, http://www.seic.gov.do/baseConocimiento/TLCEEUU%20DRCAFTA/Texto%20del%20Tratado%20en%20Español/Capítulo%2014.%20Comercio%20Electrónico/DR-CAFTA%20Capítulo%2014.%20Comercio%20Electrónico.pdf y http://www.seic.gov.do/baseConocimiento/TLCEEUU%20DRCAFTA/Texto%20del%20Tratado%20en%20Español/Capítulo%2020.%20Solución%20de%20Controversias/DR-CAFTA%20Capítulo%2020.%20Solución%20de%20Controversias.pdf
2. Procedimiento de acreditación de Entidades de Certificación de Firma Digital de los Estados Unidos de América. http://www.indotel.gob.do/component/option,com_docman/task,doc_download/gid,281/
3. Reglamento de Sistemas de Pago. http://www.bancentral.gov.do/normativa/normas_vigentes/financieros/sistemas_de_pago.pdf
4. Instructivo para la autorización y operación de las plataformas electrónicas de negociación de divisas. http://www.bancentral.gov.do/normativa/normas_vigentes/monetarios/Inst_plataforma_electronica_divisas.pdf
5. Sistema Integrado de Ventanilla Única de Comercio Exterior (SIVUCEX). http://www.sivucex.gov.do/pdf/DECRETO_248-98_SIVUCEX.pdf
6. Ley 126-02 sobre comercio electrónico, documentos y firma digital. http://www.indotel.gob.do/component/option,com_docman/Itemid,587/task,doc_download/gid,68/
7. Acuerdo de Asociación Económica entre los Estados del CARIFORUM y la Comunidad Europea y sus Estados miembros. http://www.seic.gov.do/comercioexterior/Acuerdo%20AAE%20o%20EPA%20en%20ingls/Texto%20en%20español%20EPA%20octubre08.pdf
8. Ley Monetaria y Financiera No. 183-02, artículo 56, literal b). http://www.bancentral.gov.do/normativa/leyes/Ley_Monetaria_y_Financiera.pdf
9. Ley 288-05 sobre regulación de las sociedades de información crediticia y de protección al titular de la información. http://www.datacredito.com.do/s_ley_buro.asp
10. Ley 20-00 sobre propiedad industrial. http://onapi.gob.do/pdf/ley20-00.pdf
11. Ley 65-00 sobre derecho de autor. http://www.marranzini.com/PDF/leyes/Ley65-00_Sobre_Derecho_de_Autor.pdf y http://www.seic.gov.do/baseConocimiento/TLCEEUU%20DRCAFTA/Documentos%20Legales%20Aprobados%20para%20Puesta%20en%20Marcha%20Tratado/Propiedad%20Intelectual/Ley-02-07%20modifica%20el%20art%C3%ADculo%204%20de%20la%20ley%20493.pdf
12. Ley 19-2000 sobre Mercado de Valores. http://www.hacienda.gov.do/legislacion/ley_incentivos_tributarios/Ley%2019-00%20sonbre%20Mercado%20de%20Valores.pdf.
13. Ley 358-05 Ley General de Protección al Consumidor. http://www.indotel.gob.do/component/option,com_docman/task,doc_download/gid,1410/Itemid,587/
14. Norma sobre la protección de los derechos de los consumidores y usuarios. http://www.indotel.gob.do/component/option,com_docman/task,doc_download/gid,146/
15. Norma sobre procedimientos de autorización y acreditación de los sujetos regulados. http://www.indotel.gob.do/component/option,com_docman/task,doc_download/gid,165/

16. Comisión Nacional para la Sociedad de la Información y el Conocimiento (CNSIC). http://www.cnsic.org.do/
17. Plan Estratégico E-Dominicana 2007-2010. http://www.cnsic.org.do/media/plan_edominicana/LinkedDocuments/Plan-Estrategico-E-Dominicana-2007-2010-v1(Final).pdf.
18. Ley de Rectificación Tributaria, No. 495-06. http://www.dga.gov.do/dgagov.net/uploads/file/leyes/Ley_495-06_rectificacion_fiscal.pdf.

UNITED NATIONS