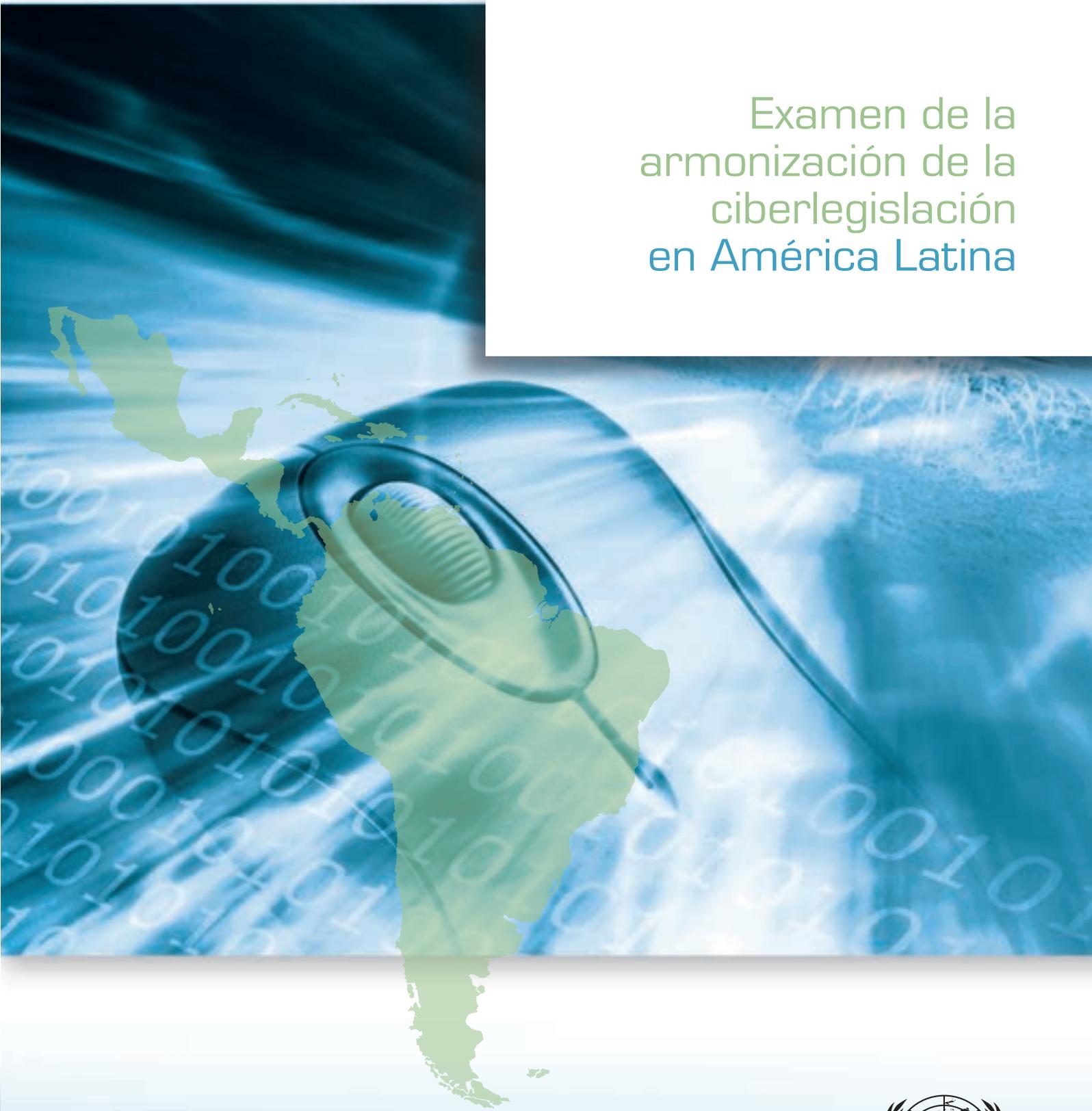




Examen de la  
armonización de la  
ciberlegislación  
en América Latina





# Examen de la armonización de la ciberlegislación en América Latina



## NOTA

Las firmas de los documentos de las Naciones Unidas se componen de letras mayúsculas y cifras. La mención de una de estas firmas indica que se hace referencia a un documento de las Naciones Unidas.

Las denominaciones empleadas en esta publicación y la forma en que se presentan los datos que contiene no implican, de parte de la Secretaría de las Naciones Unidas, juicio alguno sobre la condición jurídica de países, territorios, ciudades o zonas, o de sus autoridades, ni respecto de la delimitación de sus fronteras o límites.

El material contenido en esta publicación puede ser citado o reproducido sin restricciones, siempre que se indique la fuente y se haga referencia al número del documento. Un ejemplar de la publicación en que aparezca el material citado o reproducido deberá remitirse a la secretaria de la UNCTAD, Palais des Nations, CH-1211, Ginebra 10, Suiza.

La presente publicación fue objeto de edición externa.

## AGRADECIMIENTOS

El estudio fue preparado en el marco del trabajo del servicio Ciencia, Tecnología y TIC y el programa Train-ForTrade de la División de Tecnología y Logística de la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD).

Fue elaborado bajo la supervisión del equipo de la UNCTAD, compuesto por Gonzalo Ayala Borda, Cécile Barayre y María Luz Jaureguiberry, siendo el consultor principal encargado de la redacción del estudio el Sr. Jorge Navarro Isla. Quisiéramos agradecer los aportes realizados por los y las participantes en el “Curso de Formación a Distancia sobre los Aspectos Legales del Comercio Electrónico para América Latina y el Caribe”, llevado a cabo en junio de 2014 y, en particular, la importante contribución a la realización de este informe de aquellas personas que participaron en el “Taller Regional sobre la armonización de la ciberlegislación para el comercio electrónico en América Latina y el Caribe”, que tuvo lugar en Guayaquil (Ecuador) en septiembre de 2014: Analía Aspis, Angélique Codd, Carlos Fernando Escóbar Revollo, Nicolás Schubert, Paola Andrea Arango Henao, Salomé Vega Morera, Madelyn Rodríguez Lara, Hernán Gustavo González López, Salomón Eduardo Custodio González, Aracely Amaya Fabian, Elide Gina Tassy Cherubin, Karina Elizabeth Aquino Valle, Peter Bailey, Jonathan López Torres, Idelvía María Campos Urbina, Rafael Jesús Quintero Yau, María Luján Ojeda Chamorro, Katia Janeth Núñez Portal de Vásquez, María Elena Ferrer Lovera, Sara Patnella, Julissa Cruz y Julio Enrique Nieto Conde.

Asimismo, contribuyeron generosamente con relevantes aportes Adrián Carballo, Alfredo Reyes Krafft, Erick Rincón, Karina Medinaceli, Moisés Fraguera, Natalia Enciso, Olga Cavalli, Patricia Stanley, Belisario Contreras, Rudy Orjales, Eduardo Pizarro, Gloria Cañas, Silvia Hernández, Fiorella Niro, Gabriela Slack, Rocío Martínez Houssay, Iván Rivadeneyra, Leonardo Otatti y Carlos Vera Quintana.

La portada fuera realizada por Nadège Hadjémian. Ion Dinca se ocupó de la maquetación electrónica y Caridad Ríos preparó el texto para su publicación.

La UNCTAD agradece el apoyo financie o aportado por el Gobierno de Finlandia.

## PRÓLOGO

Con la evolución de las TICs y en particular, el desarrollo en la utilización de dispositivos móviles y el desarrollo de Cloud-computing y big data, los aspectos de seguridad tales como la protección de datos; el cibercrimen y la protección del consumidor son esenciales para la confianza de los usuarios del comercio electrónico. Asimismo, los actores involucrados en el diseño y la implantación de las políticas públicas se encuentran enfrentados a desafíos de tipo legislativo, técnicos-administrativo, de instrumentación y armonización propios de las dinámicas de sus países y de la región.

La presente publicación tiene por objeto actualizar la información sobre el marco jurídico de los países en la región, como seguimiento a los Estudios sobre las perspectivas de la armonización de la ciberlegislación en América Latina y en Centroamérica y el Caribe publicado en 2009 y 2010. El estudio informa sobre los avances realizados por los países en materia de transacciones electrónicas/firmas electrónicas; protección en línea al consumidor; protección de datos personales; propiedad industrial e intelectual; nombres de dominio; delitos informáticos y seguridad de la información, e iniciativas de ley y retos. Cabe destacar que la publicación no sólo examina la situación de 20 países de la región, sino que además brinda información relativa a los compromisos y responsabilidades asumidos en cada país en torno a la ciberlegislación tomando en cuenta el contexto regional, permitiendo de esta manera identificar las diferentes instancias de colaboración existentes, sus implicancias, limitaciones y desafíos. La publicación también hace referencia a la pluralidad de organismos en la región que han generado una amplia gama de instrumentos normativos y de políticas públicas y, a la necesidad de coordinación al interior de los gobiernos de los países en la región para avanzar en estos temas. Por ello, el estudio es un instrumento útil para los funcionarios de los gobiernos implicados en el diseño e implementación de marcos jurídicos favorables al desarrollo.

Desde 2003, la UNCTAD ha desarrollado actividades de cooperación y asistencia técnica con gobiernos de países en desarrollo en África, Asia, y América Latina, a fin de contribuir en la preparación de los marcos jurídicos que regulen el uso de las TIC. La UNCTAD ofrece capacitación en materia de aspectos jurídicos ligados a las tecnologías de la información y de las comunicaciones y apoya el proceso de elaboración de un marco legal armonizado que propicia la creación de entornos que permita el uso de las TIC en los países en desarrollo. En este sentido, la UNCTAD ha desarrollado desde 2007 diversas actividades conjuntamente a la Secretaría General de la Asociación Latinoamericana de Integración (ALADI), el Sistema Económico Latinoamericano y del Caribe (SELA), y desde 2014 también con la Asociación de Estados del Caribe (AEC), para fortalecer las capacidades de los países, compartir las experiencias regulatorias e incentivar el desarrollo de grupos de trabajo multidisciplinarios y especializados en los aspectos legales del comercio electrónico.

---

# ÍNDICE

<b>PRÓLOGO.....</b>	<b>iv</b>
<b>I. INTRODUCCIÓN .....</b>	<b>1</b>
A. ESTADO DE LA CIBERLEGISLACIÓN DE LOS PAÍSES DE AMÉRICA LATINA.....	2
B. UNA PLURALIDAD DE INICIATIVAS PARA FOMENTAR LAS OPERACIONES DE COMERCIO INTERNACIONAL EN LA REGIÓN.....	6
<b>II. REPORTE NORMATIVO DE LOS PAÍSES DE AMÉRICA LATINA.....</b>	<b>11</b>
ARGENTINA .....	11
BOLIVIA .....	14
BRASIL .....	16
CHILE .....	19
COLOMBIA.....	23
COSTA RICA.....	26
CUBA.....	28
ECUADOR .....	30
EL SALVADOR.....	33
GUATEMALA .....	37
HAITÍ .....	40
HONDURAS.....	41
MÉXICO .....	44
NICARAGUA .....	47
PANAMÁ.....	51
PARAGUAY.....	53
PERÚ .....	57
REPÚBLICA DOMINICANA.....	61
URUGUAY.....	65
VENEZUELA .....	68



## I. INTRODUCCIÓN

La reforma de la ciberlegislación constituye una piedra angular para fortalecer el desarrollo económico de los países y de la región. Asimismo, permite promover el comercio nacional y transfronterizo, incluyendo a las entidades gubernamentales de los diferentes niveles de gobierno, a las empresas y/o personas con actividades empresariales, así como a los consumidores y/o ciudadanos.

En América Latina, el comercio electrónico B2C ha aumentado en la última década, de 1,6 mil millones a 70 mil millones de dólares estadounidenses, sin embargo la región sigue desempeñando un papel menor desde una perspectiva global.<sup>1</sup>

De conformidad con el cuadro 1, Índice de Comercio Electrónico B2C de la UNCTAD,<sup>2</sup> que refleja la

capacidad subyacente de los países para llevar a cabo el comercio electrónico B2C, Chile, Uruguay y Brasil ocupan los primeros puestos en la región, ocupando Chile el primer puesto en América Latina y el puesto 39 a nivel mundial.

La ciberlegislación favorece las condiciones para lograr un entorno seguro y confiable caracterizado por la transparencia, el respeto a la privacidad, la protección de datos, la seguridad jurídica, la libertad de expresión, la libertad de consumo y de empresa. Si bien es cierto que la reforma de la ciberlegislación, en cuanto al comercio electrónico, tiende a ser una constante en los distintos países de la región, también es cierto que no figura claramente como una prioridad regional, por lo que los niveles de desarrollo normativo son heterogéneos entre los distintos países.

La presente publicación tiene por objeto actualizar los anteriores Estudios sobre las perspectivas de la armonización de la ciberlegislación en América Latina (2009)<sup>3</sup> y en Centroamérica y el Caribe<sup>4</sup> en los rubros

<sup>1</sup> eMarketer, 2014.

<sup>2</sup> Informe sobre la Economía de la Información 2015 de la UNCTAD. El índice de la UNCTAD refleja la información sobre 130 países; no cuenta con información relativa a Cuba.

**Cuadro 1. Índice de Comercio Electrónico B2C de la UNCTAD, 2015**

Economía	Proporción de la población que recibe correo en el hogar (2012 o posterior, en %)	Proporción de personas que tienen tarjeta de crédito (15+, 2011, en %)	Proporción de personas que usan Internet (2013 o posterior, en %)	Servidores seguros por cada millón de personas (normalizado en 2013)	Valor del Índice de Comercio Electrónico de la UNCTAD	Categoría
Chile	94	22,8	61,4	73,9	63,0	39
Uruguay	93	27,1	58,0	72,1	62,5	40
Brasil	81	29,2	58,0	69,9	59,5	47
Argentina	93	21,9	54,1	67,6	59,1	48
Costa Rica	98	12,2	47,5	72,5	57,6	52
República Dominicana	99	12,2	45,0	61,5	54,5	57
México	91	13,0	43,5	63,7	52,8	60
República Bolivariana de Venezuela	93	10,4	44,1	56,6	51,0	63
Colombia	60	10,2	51,27	65,6	46,9	71
El Salvador	95	5,3	25,5	60,9	46,7	72
Ecuador	68	10,2	35,1	63,0	44,1	76
Guatemala	95	6,9	16,0	58,1	44,0	77
Perú	56	10,0	38,2	61,9	41,5	82
Panamá	25	10,7	45,2	73,5	38,6	84
Honduras	75	5,3	18,1	55,1	38,4	85
Nicaragua	44	2,5	13,5	54,4	28,6	98
Bolivia	19	4,1	34,2	54,9	28,1	99
Haití	40	1,8	9,8	37,7	22,3	107

Fuente: UNCTAD, 2015.

<sup>3</sup> Véase: [http://unctad.org/es/Docs/webdtlktcd20091\\_sp.pdf](http://unctad.org/es/Docs/webdtlktcd20091_sp.pdf)

<sup>4</sup> Véase: [http://unctad.org/es/docs/dtlstict20093\\_sp.pdf](http://unctad.org/es/docs/dtlstict20093_sp.pdf)

siguientes: a) Transacciones electrónicas/firmas electrónicas<sup>5</sup>; b) Protección al consumidor; c) Protección de datos personales; d) Propiedad industrial e intelectual; e) Nombres de dominio; f) Delitos informáticos y Seguridad de la información<sup>6</sup>, g) Iniciativas de Ley y retos.

Los estudios fueron preparados con el objeto de brindar una perspectiva regional sobre el estado de la ciberlegislación en los países miembros de la Asociación Latinoamericana de Integración (ALADI) y de la subregión centroamericana, del Sistema Económico Latinoamericano y del Caribe (SELA) y de la Asociación de Estados del Caribe (AEC), que participaron activamente en los distintos programas de capacitación de la UNCTAD, de 2007 a 2014.

En ambos estudios se destaca la existencia de una pluralidad de organismos internacionales (tanto multilaterales como regionales y subregionales) que han generado una amplia gama de instrumentos normativos y de políticas públicas, conformando un complejo mosaico regulador en el que un mismo país puede estar obligado a cumplir con disposiciones emanadas de diferentes organismos, generando de esta manera: i) tensiones por incompatibilidad de algunos cuerpos normativos; ii) desarrollos dispares de regulación, leyes y políticas públicas; iii) duplicidad de esfuerzos; iv) ausencia de liderazgo y coordinación a nivel de los organismos internacionales, y v) carencia de coordinación al interior de los gobiernos de los países.

**Cuadro 2. Estado de la ciberlegislación de los países de América Latina, 2015**

País	Transacciones electrónicas/ firmas electrónicas	Protección al Consumidor	Protección de Datos	Propiedad Intelectual	Nombres de dominio	Delitos Informáticos y Seguridad de la Información
Argentina						
Bolivia						
Brasil						
Chile						
Colombia						
Costa Rica						
Cuba						
Ecuador						
El Salvador						
Guatemala						
Haití						
Honduras						
México						
Nicaragua						
Panamá						
Paraguay						
Perú						
República Dominicana						
Uruguay						
Venezuela						

Fuente: UNCTAD, 2015.

<sup>5</sup> Con la finalidad de simplificar la presentación de los resultados, en el rubro "Transacciones electrónicas/firmas electrónicas" se incluyeron los apartados siguientes de anteriores Estudios: "Transacciones Electrónicas", "Firmas Electrónicas" e "Impuestos y Aduanas".

<sup>6</sup> Por la relevancia del tema, se añadió el rubro de "Seguridad de la información" a la de "Delitos informáticos", de manera que quedaron integrados en el mismo rubro ambos conceptos: "Delitos informáticos y Seguridad de la información".

## A. ESTADO DE LA CIBERLEGISLACIÓN DE LOS PAÍSES DE AMÉRICA LATINA

En el cuadro 2 se dan a conocer los avances realizados en los diferentes países de la región<sup>7</sup>, a través del marco normativo que se describe más adelante. Los avances más notables se centran primordialmente en

<sup>7</sup> En el cuadro 2 no se han incluido iniciativas de Ley ni anteproyectos de Ley y/o reglamentos.

**Valores Normativos:**

Valor	Enunciado	Descripción
	Facilita el comercio electrónico	La legislación es acorde con las mejores prácticas internacionales acordadas por organismos internacionales, tales como la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), la Organización Mundial de la Propiedad Intelectual (OMPI), la Organización Mundial del Comercio (OMC), la Unión Internacional de Telecomunicaciones (UIT), la Red Iberoamericana de Protección de Datos Personales, el Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA) / Comité Interamericano contra el Terrorismo (CICTE), el Consejo de Europa y la Organización para la Cooperación y el Desarrollo Económicos (OCDE).
	Facilita parcialmente el comercio electrónico.	Existe legislación en la materia, sin embargo, no es acorde con las mejores prácticas internacionales. Hace falta homologación normativa.
	No existe legislación.	

las áreas de transacciones electrónicas/firmas electrónicas y de protección de datos personales; se han realizado pocos avances, principalmente en las áreas de Delitos informáticos y Seguridad de la información y, en menor medida, en relación con los Nombres de Dominio y la Protección al Consumidor.

**TRANSACCIONES ELECTRÓNICAS/FIRMAS ELECTRÓNICAS**

La adopción de normativa en materia de Transacciones Electrónicas/Firmas Electrónicas prácticamente se ha dado en la mayor parte de los países de la región: en 19 países se cuenta ya con legislación en la materia; en 16 de ellos se han incorporado disposiciones conformes con la Ley Modelo sobre Comercio Electrónico y con la Ley Modelo sobre las Firmas Electrónicas de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI); en 3 países, la normativa no aplica dichas leyes modelo y en un país no se ha emitido legislación en la materia.

Cabe señalar que, con el Proyecto de Certificado de Origen Digital de la ALADI, Argentina, Bolivia, Brasil, Cuba, Chile, Colombia, Ecuador, México, Panamá, Paraguay, Perú, Uruguay y Venezuela han logrado importantes avances en el manejo de certificados de origen en formato digital para el comercio transfronterizo.

Es importante destacar que Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua, Panamá y República Dominicana han realizado notables progresos a nivel subregional con respecto a la instrumentación del Código Aduanero Único Centroamericano (CAUCA) y el Reglamento del CAUCA, así como con la suscripción del Tratado de Libre Comercio entre la República Dominicana, Centroamérica y Estados Unidos (CAFTA- RD).

A nivel del Mercado Común del Sur (MERCOSUR), la Resolución N° 37/06 - Reconocimiento de la eficacia jurídica del documento electrónico, la firma electrónica y la firma electrónica avanzada en el ámbito del MERCOSUR y la Resolución N° 34/06 - Directrices para la celebración de acuerdos de reconocimiento mutuo de firmas electrónicas avanzadas en el ámbito del MERCOSUR han permitido la adopción de los medios electrónicos en las operaciones aduanales de Argentina, Brasil, Paraguay, Uruguay, Venezuela y Bolivia. De igual forma, con la Decisión 571 – Valor en Aduana de las Mercancías Importadas de la Comunidad Andina, Bolivia, Colombia, Ecuador y Perú han impulsado el uso de firmas digitales en las declaraciones electrónicas ante las aduanas de los países miembros.

**PROTECCIÓN AL CONSUMIDOR**

En cuanto a la Protección al Consumidor, en 18 países se han promulgado leyes, 11 de los cuales han aplicado la Resolución 39/248 sobre las Directrices para la Protección al Consumidor, aprobada por la Asamblea General de las Naciones Unidas, y en 2 países no se han promulgado leyes en la materia ni se cuenta con proyectos de Ley.

A nivel del MERCOSUR, la Resolución N° 21/04 - Derecho a la Información del Consumidor en las Transacciones Comerciales efectuadas a través de Internet, la Resolución del MERCOSUR N° 45/06 - Defensa del Consumidor - Publicidad Engañosa y el Decreto N° 10/96 - Protocolo de Santa María MERCOSUR 10/96 sobre Jurisdicción Internacional en materia de relaciones de consumo han facilitado la armonización normativa sobre esos temas para Argentina, Brasil, Paraguay, Uruguay, Venezuela y Bolivia.

Adicionalmente, en el ámbito de la autorregulación, diversas cámaras y asociaciones nacionales han desarrollado Códigos de Conducta y esquemas de

### Recuadro 1. Iniciativa eConfianza y eResolución del Instituto Latinoamericano de Comercio Electrónico (eInstituto)

La iniciativa eConfianza del Instituto Latinoamericano de Comercio Electrónico (eInstituto) se ha sumado a los esfuerzos de la Cámara Argentina de Comercio Electrónico (CACE), la Cámara de Comercio de Santiago (CCS), la Cámara Venezolana de Comercio Electrónico (CAVECOM-E), la Cámara Brasileira de Comercio Electrónico (Cámara e-net), la Asociación Mexicana de Internet (AMIPCI), la Cámara Paraguaya de Comercio Electrónico (CAPACE), la Cámara Peruana de Comercio Electrónico (CAPECE), la Cámara Dominicana de Comercio Electrónico Inc. (CADOLEC), la Cámara de Comercio de Lima (CCL), la Cámara Colombiana de Comercio Electrónico (CCCE), la Cámara de Comercio de Guayaquil (CCG) y la Corporación Ecuatoriana de Comercio Electrónico (CORPECE), las cuales cuentan con un sistema de reconocimiento cruzado de sellos de confianza

Cabe señalar que, tanto el Sello de Confianza e-Confianza como el Sello de Confianza de la AMIPCI participan en la Red Mundial de Sellos (World Trust Mark Alliance), que comprende 12 esquemas de sellos de confianza de países asiáticos, 6 de países europeos y el Trust de los Estados Unidos de Norteamérica. Mediante la iniciativa eResolución del eInstituto, se está desarrollando un Programa Piloto de Resolución Electrónica de Disputas en eConfianza (para disputas derivadas del Comercio y los Negocios Electrónicos) que favorece la participación de eConfianza como Tercero Neutral Online y que busca fomentar las experiencias positivas en línea para lograr el crecimiento y afianzamiento de la economía digital en la región<sup>8</sup>.

Fuente: eInstituto, 2014.

Sellos de Confianza relacionados con el comercio electrónico (véase el recuadro 1). La participación de los países centroamericanos en el CAFTA-RD y el Tratado de Promoción Comercial entre Panamá y Estados Unidos ha permitido incentivar la adopción de este tipo de mecanismos.

Algunos países, como México y Chile, ya habían incorporado en su normativa interna las Directrices para la Protección de los Consumidores en el Contexto del Comercio Electrónico (1999) y las Directrices de la OCDE para la Protección de los Consumidores de Prácticas Comerciales Transfronterizas, Fraudulentas y Engañosas. De igual forma, habían participado en el proyecto "Pathfinder de privacidad" del Foro de Cooperación Económica Asia-Pacífico (APEC).

## PROTECCIÓN DE DATOS PERSONALES

La mayoría de los países han adoptado leyes en materia de Protección de Datos Personales: en 19 países ya se han promulgado leyes, siendo diez los países que observan las Directrices formuladas por la Red Iberoamericana de Protección de Datos; en un país no se han promulgado leyes en la materia ni cuenta con proyectos de ley.

## PROPIEDAD INTELECTUAL

En cuanto a la Propiedad Intelectual, la totalidad de los países han suscrito la mayoría de los Tratados

administrados por la OMPI, y solamente dos no han suscrito los "Tratados Internet".

Entre los avances más representativos en la región, es preciso mencionar el caso de Chile con su Ley N° 20.435 que modifica la Ley sobre Propiedad Intelectual (Ley N° 17.336), la cual incorpora por primera vez en la región el régimen de "Puerto Seguro", limitado a los temas autorales, en el que instrumenta un procedimiento de "notificación y retiro judicial" y un apartado dedicado al procedimiento judicial sumario que se debe seguir para solicitar el retiro de materiales infractores. De igual forma, Costa Rica incorpora en el Decreto N° 36880-COMEX-JP, Reglamento sobre la limitación a la responsabilidad de los proveedores de servicios por infracciones a Derechos de Autor y Conexos, un esquema de excluyentes de responsabilidad para los prestadores de servicios. Por su parte Paraguay, en virtud de la Ley sobre Comercio Electrónico (Ley N° 4.868/13), incorpora un régimen de exclusión de responsabilidad para los proveedores de los servicios de intermediación, alojamiento de datos, enlaces y de copia temporal.

En el ámbito internacional, la suscripción del Tratado de Beijing sobre Interpretaciones y Ejecuciones Audiovisuales (2012) de la OMPI<sup>9</sup> ha sido uno de los puntos más relevantes, debido a la amplia aceptación del mismo en los Estados de la región, pues lo han firmado Chile, Colombia, Costa Rica, El Salvador, Guatemala, Haití, Honduras, Jamaica, México, Nicaragua y Perú. Sin embargo, su entrada en

<sup>8</sup> Véase: <http://www.einstituto.org/site/iniciativas/eresolucion/>

<sup>9</sup> Véase: [http://www.wipo.int/treaties/es/text.jsp?file\\_id=295839](http://www.wipo.int/treaties/es/text.jsp?file_id=295839)

vigor tendrá lugar tres meses después de que treinta Partes, que reúnan las condiciones mencionadas en el artículo 23, hayan depositado sus instrumentos de ratificación o adhesión.

### **NOMBRES DE DOMINIO**

En cuanto a los Nombres de Dominio, los registradores nacionales de 18 países han adoptado la normativa referente a la solución de controversias, 12 de los cuales recogen los principios de la Política uniforme de solución de controversias de la Corporación para la Asignación de Nombres y Números de Internet (ICANN, por sus siglas en inglés) y uno no cuenta con instrumentos normativos en la materia.

Los procedimientos de solución de controversias que aplica el Centro de Información de Red (NIC) de Haití se apartan de la Política uniforme de solución de controversias en materia de nombres de dominio de la ICANN.

La coordinación de las autoridades registradoras de la región por conducto del Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC), bajo la coordinación global de la ICANN, constituye una de las piedras angulares que permiten el desarrollo de Internet en Latinoamérica, Centroamérica y el Caribe. En este sentido, la adopción de la Política uniforme de solución de controversias en materia de nombres de dominio establecida por la ICANN resulta de máxima trascendencia para uniformar los criterios de las autoridades registradoras a nivel regional.

En materia de nombres de dominio, tanto el NIC Argentina como el NIC Chile, NIC México, NIC Perú y NIC Venezuela han adoptado, en el marco de sus políticas de solución de controversias, la Política uniforme de solución de controversias en materia de nombres de dominio de la ICANN, y reconocen el procedimiento arbitral del Centro de Arbitraje y Mediación de la OMPI. En el caso de Perú, también se reconoce como instancia arbitral al Cibertribunal Peruano. Por su parte, el NIC Paraguay dirime sus controversias sobre nombres de dominio mediante mecanismos extrajudiciales regidos por la Ley N° 1.879/02 de Arbitraje y Mediación.

Adicionalmente, el CAFTA-RD obliga a los países miembros a establecer mecanismos para combatir la piratería cibernética mediante la instrumentación de procedimientos basados en los principios de la Política uniforme de solución de controversias. Sobre el particular, los procedimientos de solución de controversias utilizados por el NIC de Costa Rica, El Salvador, Honduras y República Dominicana se

apartan de la Política uniforme de solución de controversias en materia de nombres de dominio de la ICANN, cuestión que puede inhibir el desarrollo de negocios transfronterizos en la región.

### **CIBERDELITOS**

Por lo que respecta a los ciberdelitos, dos países han suscrito el Convenio del Consejo de Europa sobre la Ciberdelincuencia y han modificado sus leyes sustantivas y procesales de conformidad con ese instrumento; en 17 países hay leyes que tipifican algunos delitos informáticos y, en uno, no hay normativa alguna. Respecto de la Seguridad de la Información son 13 los países que tienen un Centro de Respuesta a Incidentes Cibernéticos (CSIRT, CERT o CIRT) y que han adoptado las recomendaciones del Comité Interamericano contra el Terrorismo (CICTE) de la Organización de los Estados Americanos (OEA)<sup>10</sup>.

A nivel subregional, desde 2012 la Unión de Naciones Suramericanas (UNASUR)<sup>11</sup> ha venido trabajando en Planes de Acción anuales del Consejo de Defensa Suramericano<sup>12</sup>, en virtud de los cuales ha conformado un Grupo de Trabajo para evaluar la factibilidad de establecer políticas y mecanismos regionales a fin de hacer frente a las amenazas cibernéticas o informáticas en el ámbito de la defensa. En 2013, el Grupo de Trabajo realizó un Seminario Regional de Ciberdefensa con el objetivo de generar capacidades para enfrentar los desafíos de las amenazas cibernéticas e informáticas del ámbito de la defensa. Participaron en este Seminario el Consejo Suramericano de Infraestructura y Planeamiento (COSIPLAN) y el Grupo de trabajo sobre Telecomunicaciones del MERCOSUR.

En 2014, la Conferencia de Ministros de Justicia de los Países Iberoamericanos (COMJIB)<sup>13</sup> suscribió el

<sup>10</sup> <http://www.oas.org/es/sms/cicte/documentos.asp>

<sup>11</sup> UNASUR es un organismo internacional, conformado por los doce países de la región suramericana: Argentina, Bolivia, Brasil, Colombia, Chile, Ecuador, Guyana, Paraguay, Perú, Surinam, Uruguay y Venezuela. El objetivo de UNASUR consiste en construir un espacio de integración en lo cultural, económico, social y político, respetando la realidad de cada nación.

<sup>12</sup> Véanse el Plan de Acción 2012 del Consejo de Defensa Suramericano: <http://www.ceedcds.org.ar/Espanol/09-Downloads/Esp-PA/Plan-de-Accion-2012.pdf>; el Plan de Acción 2013 del Consejo de Defensa Suramericano: <http://www.ceedcds.org.ar/Espanol/09-Downloads/Esp-PA/Plan-de-Accion-2013.pdf> y el Plan de Acción 2014 del Consejo de Defensa Suramericano: <http://www.ceedcds.org.ar/Espanol/09-Downloads/Esp-PA/Plan-de-Accion-2014.pdf>

<sup>13</sup> La COMJIB agrupa a los Ministerios de Justicia e instituciones homólogas de Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, España, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Portugal, República Dominicana, Uruguay y

Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia, que tiene por objeto reforzar la cooperación mutua de las Partes para la adopción de medidas de aseguramiento y obtención de pruebas para la lucha contra la ciberdelincuencia, así como la Recomendación relativa a la Tipificación y Sanción de la Ciberdelincuencia. Los instrumentos han sido suscritos por México, Guatemala, Nicaragua, Portugal, Perú y Uruguay y firmado por Argentina

Los instrumentos precitados representan el mayor avance regional en cuanto a la atención señalada a esta problemática. Derivado de las carencias que las leyes penales iberoamericanas tienen respecto de los tipos penales referidos al ciberdelito, y al hecho de que estas lagunas permiten tanto a la delincuencia individual como a la organizada lesionar o poner en grave peligro los bienes jurídicos esenciales con el propósito de establecer criterios mínimos y comunes en la prevención y luchas contra el ciberdelito, y sin menoscabar los avances alcanzados en los respectivos ordenamientos jurídicos así como las obligaciones internacionales asumidas por cada Estado, la COM-JIB recomienda armonizar, en el marco de las políticas criminales de cada país, leyes penales sustantivas que tipifiquen las conductas que se describen a continuación, en aras de lograr una mayor eficacia en la prevención, persecución y sanción de dichos ilícitos para facilitar la cooperación judicial entre los distintos países y tratar de impedir la existencia de espacios de impunidad. El Convenio es compatible con otros instrumentos internacionales, como el Convenio del Consejo de Europa sobre la Ciberdelincuencia.

Merece especial mención la “Declaración Especial 15: Sobre procesos de gobernanza en Internet”<sup>14</sup>, adoptada durante la III Cumbre de la Comunidad de Estados Latinoamericanos y Caribeños (CELAC)<sup>15</sup>, celebrada en Belén (Costa Rica), en enero de 2015, en la que Jefes y Jefes de Estado y de Gobierno de

los treinta y tres Estados de la región manifestaron lo siguiente: i) la aspiración de convertir a América Latina y el Caribe en una región de redes de conocimiento<sup>16</sup>; ii) su condena decidida contra las acciones de espionaje y vigilancia masiva y global indiscriminada entre los países por parte de actores públicos y privados, exigiendo absoluto acatamiento a las normas del derecho internacional, en relación con el respeto a la soberanía de los estados y a los derechos humanos, en especial el derecho a la privacidad<sup>17</sup>, y iii) su compromiso para promover acciones y estrategias para fortalecer la ciberseguridad y prevenir los delitos informáticos, articulando mecanismos para la erradicación de la guerra cibernética y la promoción de Internet como un espacio de paz<sup>18</sup>.

## B. UNA PLURALIDAD DE INICIATIVAS PARA FOMENTAR LAS OPERACIONES DE COMERCIO INTERNACIONAL EN LA REGIÓN

El marco legal que sustenta el comercio electrónico para la reforma de la ciberlegislación ha permeado las Agendas Digitales de varios países de la región, cuyos marcos normativos se analizan en el presente Estudio. La normativa que rige las operaciones comerciales en línea, apoyadas en el uso de infraestructura de llave pública y certificados digitales que incentivan la interoperabilidad de las plataformas en un contexto seguro, incluso a través de esquemas tecnológicos de cómputo en la nube y que permiten lograr los beneficios de las economías de escala, es una realidad en varios países de la región.

Tanto el Estudio sobre las perspectivas de la armonización de la ciberlegislación en América Latina (2009) como el Estudio sobre las perspectivas de la armonización de la ciberlegislación en Centroamérica y el Caribe (2010) reportaron como avances más significativos la adopción de los compromisos de los Planes de Acción sobre la Sociedad de la Información en América Latina y el Caribe de 2008 y 2010 (Plan eLAC 2010 y Plan eLAC 2015), que tienen a la Comisión Económica para América Latina y el Caribe (CEPAL) como Secretaría Técnica. La mayoría de los países define on metas comunes a nivel regional que han incidido en el desarrollo del comercio electrónico así como en las actividades de gobierno electrónico,

Venezuela. Véase el enlace siguiente: <http://www.comjib.org/documentos>

<sup>14</sup> Disponible en: <http://celac.mmrree.gob.ec/index.php/es/docu-base-menu/declaracion-de-belen.html>

<sup>15</sup> CELAC es un mecanismo intergubernamental de diálogo y concertación política que reúne de forma permanente a los treinta y tres países de América Latina y el Caribe. Forman parte de la CELAC los siguientes países: Antigua y Barbuda, Argentina, Bahamas, Barbados, Belice, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Dominica, Ecuador, El Salvador, Granada, Guatemala, Guyana, Haití, Honduras, Jamaica, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, San Cristóbal y Nieves, Santa Lucía, San Vicente y las Granadinas, Surinam, Trinidad y Tobago, Uruguay y Venezuela. Fuente: <http://celac.mmrree.gob.ec/index.php/es/>

<sup>16</sup> Resolutivo número 10 de la Declaración Especial 15: Sobre procesos de gobernanza en Internet.

<sup>17</sup> Resolutivo número 2 de la Declaración Especial 15: Sobre procesos de gobernanza en Internet.

<sup>18</sup> Resolutivo número 3 de la Declaración Especial 15: Sobre procesos de gobernanza en Internet.

mediante la adopción de mecanismos que involucran el uso de firmas y certificados digitales así como la instrumentación del concepto de ventanilla única, que han resultado compatibles entre las diferentes dependencias de un mismo Estado o de los distintos Estados de la región.

Varios Estados han planteado Agendas Digitales en las cuales se propone el uso de las tecnologías de la información y las comunicaciones (TIC) como instrumentos catalizadores del desarrollo y de la inclusión social. El papel que deben desempeñar las TIC en cuanto a las relaciones entre las entidades gubernamentales y los gobernados es fundamental, e incluso países como México, Paraguay, Perú y República Dominicana han integrado de manera explícita en sus Agendas Digitales su estrategia nacional para promover el comercio electrónico.

En agosto de 2015, en el marco de la Quinta Conferencia Ministerial sobre Sociedad de la Información en América Latina y el Caribe, los países de la región aprobaron una Agenda digital regional hacia 2018 (eLAC2018). Este compromiso plantea a los Estados la conveniencia de impulsar la innovación y la competitividad mediante el fortalecimiento de la economía digital. Esta nueva agenda digital establece como objetivo potenciar la economía digital y el comercio electrónico, adaptando las regulaciones de protección al consumidor al entorno digital y coordinando aspectos tributarios, de logística y transporte, de medios de pago electrónicos y de protección de datos personales, además de brindar seguridad jurídica para promover la inversión en el ecosistema digital.

En relación con las iniciativas para las operaciones de comercio internacional en la región se puede mencionar el proyecto de Certificación de Origen Digital (COD) de la ALADI<sup>19</sup>, en el que participan Argentina,

Bolivia, Brasil, Chile, Colombia, Cuba, Ecuador, México, Panamá, Paraguay, Perú, Uruguay y Venezuela. Dicho proyecto ha favorecido la facilitación del comercio transfronterizo mediante la utilización de medios electrónicos entre esos países, particularmente en cuanto a la integración y armonización de estándares y formatos y plataformas que han permitido la interoperabilidad de los sistemas aduaneros de los distintos países.

La adopción por parte de los Estados Miembros de las Especificaciones Técnicas y Procedimientos Generales para la Certificación de Origen Digital (COD), emitidas por la Secretaría General de la ALADI en 2014, será de especial relevancia para la integración económica regional que se apoya también en el importante pilar de los acuerdos bilaterales<sup>20</sup> (véase el recuadro 2).

En el cuadro 3 se describe la situación relativa a la implementación de la última versión del COD de la ALADI.

Por su parte, el SELA también ha sido un impulsor de los Sistemas de Ventanilla Única de Comercio Exterior (VUCE) en la región, que han beneficiado a diversas economías de Latinoamérica, Centroamérica y el Caribe (véase el cuadro 4).

Como se observa, alrededor del 52% de los países de la región cuenta con algún grado de desarrollo de este instrumento. El nivel de implementación y madurez del sistema va desde países como Colombia que, desde mediados de la década pasada cuenta con una VUCE operativa, hasta Argentina, que recientemente la ha formalizado, y Nicaragua, que ha emprendido su desarrollo. La información que se ha proporcionado en el cuadro anterior procede directamente de los países de la región con quienes el SELA mantiene una actividad permanente en áreas de facilitación del comercio y específicamente en lo relativo al desarrollo de Ventanillas Únicas de Comercio Exterior.

El SELA ha desempeñado un papel destacado por su contribución en la generación del diálogo regional a través de la realización anual de los Encuentros Regionales Latinoamericanos y del Caribe sobre Ventanillas Únicas de Comercio Exterior<sup>21</sup>. Este espacio para el encuentro regional se ha constituido en un escenario privilegiado para difundir información y buenas

<sup>19</sup> Véase el Informe Final de la II Reunión de Coordinadores Nacionales en Materia de Certificación de Origen Digital en: [http://www.aladi.org/nsfaladi/reuniones.nsf/documentos/\\$file/InformeFinalCOD2014.pdf](http://www.aladi.org/nsfaladi/reuniones.nsf/documentos/$file/InformeFinalCOD2014.pdf). Respecto de la relevancia de los Acuerdos Bilaterales se enfatiza en el apartado "3. Relevamiento y seguimiento de los proyectos de cooperación técnica horizontal entre los países demandantes y oferentes en relación a la "Instrumentación del Programa de Cooperación para la implementación del COD en los países miembros de la ALADI", en el que la Coordinación de la Reunión "estimuló a los países a continuar avanzando en la cooperación horizontal con el fin de lograr la implementación de la certificación de origen digital en el plazo más breve posible, y a tales efectos se abrió el espacio destinado a la realización de reuniones bilaterales". Asimismo, en el apartado "4. Reuniones bilaterales de coordinación para facilitar la ejecución de los proyectos del Programa de Cooperación", se hace mención a que en ese espacio "se llevaron a cabo 23 reuniones bilaterales entre los países presentes", cuyos resultados se reflejan en el apartado "5. Presentación de los resultados de las reuniones bilaterales a efectos de actualizar el Documento ALADI/SEC/dt 536 de 8 de noviembre de 2013 – "Instrumentación del Programa de

Cooperación para la implementación del COD en los países miembros de la ALADI."

<sup>20</sup> Véase: Certificación de Origen Digital de la ALADI – Especificaciones Técnicas y Procedimientos Generales en: [http://foros.aladi.org/gtah/ALADI\\_SEC\\_di2327rev2.pdf](http://foros.aladi.org/gtah/ALADI_SEC_di2327rev2.pdf)

<sup>21</sup> Véanse los informes finales de los encuentros en: [www.sela.org](http://www.sela.org).

### Recuadro 2. Certificación de Origen Digital en el ámbito de la ALADI

La Certificación de Origen Digital en el ámbito de la ALADI está conformada por un conjunto de especificaciones, estándares y procedimientos técnicos, los cuales constituyen la base de una infraestructura informática, integrada por aplicaciones y documentos electrónicos, que posibilitan el reconocimiento de los COD en el ámbito de la ALADI. La descripción de las referidas especificaciones, estándares y procedimientos técnicos constituyen, por lo tanto, el contenido principal del presente documento.

Por su parte, las principales aplicaciones que conforman la Certificación de Origen Digital son: i) las de recepción de solicitudes y emisión del COD de las Entidades Habilitadas (EH); ii) las de las Aduanas para la recepción y validación de los COD en el país importador, y iii) el Sistema informático de Certificación de Origen Digi al de la ALADI (SCOD).

i. Las aplicaciones de recepción de solicitudes y emisión del COD de las EH deberán permitir que la solicitud del COD sea firmada electrónicamente por el Exportador y/o su Representante Legal. A dichos efectos, estos deberán tramitar previamente un Certificado de Identificación Digital (CID) ante la Autoridad de Certificación (AC) competente. El resultado de este proceso será un archivo en formato XML (eXtensible Markup Language) que contendrá la información requerida para tramitar la solicitud del COD, según lo establecido en el Régimen de Origen del Acuerdo correspondiente.

En este sentido, la EH deberá proveer la infraestructura informática necesaria para recibir y procesar la solicitud del COD, validar la firma digital del Exportador y/o su Representante Legal, firmar digitalmente el nuevo archivo XML que constituye el COD y emitirlo de acuerdo a lo establecido en el correspondiente Régimen de Origen.

ii. Las Aduanas deben adecuar sus sistemas informáticos para permitir la recepción y validación de los COD. El proceso de validación involucrará la realización de consultas automáticas al SCOD respecto a la información contenida en el COD.

iii. El SCOD de la ALADI es una aplicación Web, cuya función principal consiste en administrar un Directorio Seguro (DS) de Certificados de Identificación Digitales (CID) de los Funcionarios Habilitados (FH) para firmar los COD y, al mismo tiempo, brindar un servicio de consulta a las Aduanas sobre la vigencia de los FH y sus CID, durante el proceso de validación del COD al momento de la importación.

Los principales documentos electrónicos de la Certificación de Origen Digital son: el COD, los CID de los FH y de los usuarios del SCOD, que constituyen los documentos de identidad electrónica de los usuarios del SCOD y de los FH; la especificación de los mecanismos de intercambio electrónico de información, a saber, los Servicios Web y los archivos de intercambio del DS del SCOD.

Fuente: ALADI.

prácticas identificadas, tanto al interior de la región de América Latina y el Caribe como en experiencias avanzadas de otras latitudes, lo que indudablemente ha contribuido a estimular la implementación y el desarrollo de las VUCE en los países de la región.

Adicionalmente, la Secretaría Permanente del SELA ha contribuido al considerable desarrollo de la producción intelectual y la sistematización de la documentación respectiva en torno al tema de las VUCE y al comercio sin papel transfronterizo, a través del Panorama Digital de los Trámites de Comercio Exterior en América Latina y el Caribe (SELA, 2010<sup>22</sup>) y el Proyecto Piloto de Interoperabilidad y Armonización de las Ventanillas Únicas de Comercio Exterior<sup>23</sup> en el marco del Arco del Pacífico Latinoamericano, adelantado en 2012 mediante el Convenio de Cooperación con la Corporación Andina de Fomento (CAF), que incluye además documentos específicos sobre firma digital y comercio electrónico.

Desde el año 2014, también en el marco de un Convenio de Cooperación con la CAF, se ha avanzado en un Programa para la creación de la Red Latinoamericana y Caribeña de Puertos Digitales y Colaborativos

que incluye, no solo la digitalización de los procedimientos portuarios, aspectos operativos relativos a la sincronización de servicios, elementos de gobernanza y estándares de calidad, sino también la interoperabilidad de Ventanilla Única de Comercio Exterior con la Ventanilla Única Portuaria. La Secretaría Permanente del SELA contribuye con la instrumentación, el desarrollo y la consolidación de la Ventanilla Única de Comercio Exterior (VUCE) en América Latina y el Caribe, en tanto componente clave de la facilitación del comercio, con el objetivo último de generar mejores condiciones de competitividad y sustentabilidad para una mayor y más eficiente inserción de los países de esta región en un comercio internacional cada vez más globalizado.

Por su parte, el Mercado Común del Sur (MERCOSUR) y el Sistema de la Integración Centroamericana (SICA) han promovido el comercio electrónico en sus correspondientes subregiones y continúan sus esfuerzos para alcanzar una mayor integración entre los distintos organismos, a fin de lograr una mayor armonización normativa.

De igual manera, resulta de especial trascendencia que aquellos países que no han incorporado a su sistema normativo los instrumentos de la CNUDMI sobre comercio electrónico lo hagan, en particular la Convención de las Naciones Unidas sobre los Con-

<sup>22</sup> Véase: [http://sela.org/attach/258/EDOCS/SRed/2010/04/T023600004015-0-Panorama\\_Digital\\_-Tramites\\_de\\_Comercio\\_Exterior.pdf](http://sela.org/attach/258/EDOCS/SRed/2010/04/T023600004015-0-Panorama_Digital_-Tramites_de_Comercio_Exterior.pdf)

<sup>23</sup> Véase: <http://www10.iadb.org/intal/intalcdi/PE/2012/10992.pdf>

**Cuadro 3. Matriz de Implementación COD ALADI (\*\*)**

Países	1		2		3		4		5		6	7
	Desarrollo de la plataforma para emitir COD (EH)		Desarrollo de la plataforma para recibir COD (AD)		Registro oficial en el SCOD de Pruebas		Homologación Interna (Validación de la firma del COD en el SCOD)		Homologación Externa (Validación de la firma del COD en el SCOD)		Registro oficial el SCOD de producción	Producción (Validación de la firma del COD en el SCOD)
	En proceso	Concluida	En proceso	Concluida	En proceso	Concluida	En proceso	Concluida	En proceso	Concluida		
<b>Argentina</b>		X		X		X		X	X		X	
<b>Bolivia</b>	X											
<b>Brasil</b>		X		X		X		X	X		X	
<b>Chile</b>		X	X		X	X						
<b>Colombia</b>		X	X			X	X		X		X	
<b>Cuba</b>	X		X									
<b>Ecuador</b>	X		X		X							
<b>México</b>	X		X		X							
<b>Panamá</b>	X		X									
<b>Paraguay</b>	X		X									
<b>Perú (**)</b>												
<b>Uruguay</b>		X		X	X		X	X				
<b>Venezuela</b>												

\* Matriz sobre el estado de situación de la implementación del COD (versión 1.8.0) en los países miembros de la ALADI, con base en lo establecido en la Resolución 386 del Comité de Representantes.

\*\* Actualmente, Perú no tiene un proyecto de adecuación al SCOD.

Fuente: ALADI – 2015.

tratos de Compraventa Internacional de Mercaderías a través de medios electrónicos de la CNUDMI, para facilitar el comercio electrónico transfronterizo.

Los esquemas de autorregulación y los mecanismos alternativos de solución de controversias en línea representan opciones viables y eficientes para proteger los intereses de los consumidores, sea que estos cuenten con marcos normativos robustos o con marcos normativos poco desarrollados. Los sellos de confianza regionales han tenido un desarrollo creciente, aunque modesto, y constituyen alternativas que pueden incentivar el desarrollo del comercio en línea. El programa regional eConfianza del Instituto Latinoamericano de Comercio Electrónico (el Instituto) y la Cámara Argentina de Comercio Electrónico (CACE) unifican los esfuerzos regionales de 12 Cámaras y Asociaciones de comercio electrónico y en él se ha definido un estándar de buenas prácticas que facilita la adopción, el uso y el reconocimiento recíproco de los sellos de confianza y de códigos de buenas prácticas en Latinoamérica<sup>24</sup>.

Por su parte, la adopción de leyes de protección de datos que cumplan con los parámetros de las Directrices formuladas por la Red Iberoamericana de Protección de Datos contribuirá significativamente al incremento de la confianza de los consumidores en línea. Asimismo, la adhesión de los diferentes Estados al Convenio del Consejo de Europa sobre la Ciberdelincuencia así como al Convenio Iberoamericano de

Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia y la adopción de la Recomendación de la COMJIB relativa a la Tipificación y Sanción de la Ciberdelincuencia resulta deseable. De igual forma, la creación de un Centro de Respuesta a Incidentes Cibernéticos (CERT o CSIRT) en los términos de la Estrategia Interamericana Integral para Combatir las Amenazas a la seguridad cibernética del CICTE de la OEA contribuirá de manera notable a consolidar la confianza en los medios electrónicos.

<sup>24</sup> Véase: <http://www.einstituto.org/site/iniciativas/econfianza/>

<b>Cuadro 4. Desarrollo de Ventanilla Única de Comercio Exterior en países de América Latina y el Caribe (ALC) (2014)</b>			
<b>País</b>	<b>Exportaciones</b>	<b>Importaciones</b>	<b>En proceso de desarrollo</b>
Argentina	-	-	X
Brasil	X	X	
Chile	X	-	X – en proceso. Incorporación de servicios: complementar exportaciones e iniciar importaciones
Colombia	X	X	Mejoramiento continuo: inclusión de otros servicios, además de exportaciones e importaciones
Costa Rica	X	-	X – Incorporación de servicios: importaciones
Ecuador	X	X	
El Salvador	X	-	X – Incorporación de servicios: importaciones
Guatemala	X	-	
Honduras	-	-	X
México	X	X	Mejoramiento continuo: inclusión de otros servicios
Nicaragua	-	-	X
Panamá	X	-	X: en proceso. Incorporación de servicios: complementar exportaciones e iniciar importaciones
Paraguay	X	-	-
Perú	X	X	Mejoramiento continuo: inclusión de otros servicios además de exportaciones e importaciones
República Dominicana	-	-	X
Trinidad y Tobago	X	X	X – en proceso. Incorporación de otros servicios: importaciones
Uruguay	X	X	X – complementando exportaciones e importaciones

Fuente: elinstituto, 2014.

## II. REPORTE NORMATIVO DE LOS PAÍSES DE AMÉRICA LATINA

En esta sección se analiza el desarrollo normativo de cada uno de los países participantes, mediante un breve análisis de la normativa en materia de:

- a) Transacciones electrónicas/Firmas electrónicas;
- b) Protección al consumidor;
- c) Protección de datos personales;
- d) Propiedad industrial e intelectual;
- e) Nombres de dominio;
- f) Delitos Informáticos y Seguridad de la Información, e
- g) Iniciativas de Ley y retos.

### ARGENTINA

En la normativa argentina no existe una legislación específica que regule las contrataciones realizadas por vía electrónica. Sin embargo, se pueden mencionar normas dispersas en distintos ordenamientos que rigen determinados aspectos relacionados con el comercio electrónico. En el marco de los principales ordenamientos se encuentran la Ley de Firma Digital (Ley N° 25.506), del 11 de diciembre de 2001, y la Ley de Defensa del Consumidor (Ley N° 24.240), del 13 de octubre de 1993 (texto actualizado por la Ley N° 26.994, vigente a partir del 1 de agosto de 2015), el Código Civil y el Código de Comercio y el nuevo Código Civil y Comercial de la Nación, del 8 de octubre de 2014, que entrará en vigor el 1 de enero de 2016.

#### a) Transacciones electrónicas /Firmas electrónicas

El Código Civil regula diversos temas vinculados con la formación de los contratos y las formalidades que éstos deben observar. Así, el Código establece las principales normas que rigen la oferta al público y su aceptación, la formación de los contratos entre presentes y entre ausentes, así como el momento en que se perfecciona el contrato.

Por su parte, el Código de Comercio, establece respecto de las ofertas indeterminadas al público, que éstas no son vinculantes. En materia de protección al consumidor, la Ley 24.240 determina que aquellas ofertas dirigidas a los consumidores potenciales indeterminados, obligan a quienes las emiten durante el tiempo en que las realicen, debiendo proporcionar información diversa en torno a las modalidades, condiciones o limitaciones de las ofertas. Asimismo, señala que las precisiones formuladas en la publicidad también obligan al oferente y se deben tener por incluidas en el contrato con el consumidor.

En materia de transacciones electrónicas, la Ley 25.506 reconoce la eficacia jurídica del documento

electrónico, de la firma electrónica y de la firma digital. A mayor abundamiento, la Ley establece la equivalencia funcional entre la firma autógrafa y la firma digital. De igual forma, señala que los documentos digitales cumplen con el requisito de la forma escrita. Esta Ley se basa en la Ley Modelo de la CNUDMI sobre Comercio Electrónico y la Ley Modelo de la CNUDMI sobre Firmas Electrónicas y se aplica en el ámbito de los sectores público y privado.

Es preciso señalar que diversas provincias de Argentina se han adherido a esta Ley, a efectos de aplicarla en sus respectivas jurisdicciones en el ámbito administrativo. Adicionalmente, Argentina ha suscrito y ha incorporado en su normativa interna dos resoluciones del MERCOSUR respecto de los estándares sobre el uso de firmas digitales, a saber, la Resolución N° 34/06 y la Resolución N° 37/06 relativas a la firma electrónica y la firma digital

Por su parte, la Administración Federal de Ingresos Públicos (AFIP) ha emitido Resoluciones Generales que imponen cargas adicionales para quienes llevan a cabo operaciones de comercio electrónico. La Resolución General 3579 establece la obligación para quienes realizan compras de mercaderías a proveedores del exterior que ingresen al país de completar el Formulario N° 4550 (Compras a proveedores del exterior) con anterioridad al retiro o recepción de la mercadería.

Asimismo, la Resolución General 3582 de la AFIP, que complementa las disposiciones contenidas en la Resolución General 3579, y que dispone que los sujetos que compran mercaderías a proveedores del exterior que ingresen al país mediante el correo oficial –incluido el servicio puerta a puerta– solo podrán utilizar el procedimiento previsto en la RG 3579 en dos oportunidades cada año calendario, teniendo en cuenta la franquicia anual de U\$S 25 prevista en el Artículo 80, Apartado 1, Inciso c) del Decreto N° 1001/82 y sus modificaciones. En caso de que los envíos excedan el límite precitado deberán ser cursados al amparo del Régimen General de Importación.

Por su parte, la Resolución General 3377 de la AFIP ordena a los contribuyentes que vendan bienes o presten servicios a consumidores finales a que exhiban el Formulario N° 960/NM - Data Fiscal en sus locales de venta, locación o prestación de servicios, salas de espera, oficinas o áreas de recepción y a que coloquen en un lugar visible de la página principal del

sitio web el logo formulario citado con el hipervínculo provisto por la AFIP.

En torno a las contrataciones públicas por medios electrónicos, el Decreto 1023/2001 regula el régimen de contrataciones para la Administración Nacional, reglamentado mediante Decreto 1818/2006, que autoriza el uso del Sistema Electrónico de Contrataciones Públicas (SECOP). Asimismo, la Decisión Administrativa No. 6/2007 de la Jefatura de Gabinete de Ministros establece las normas técnicas para la operación de la Infraestructura de Firma Digital de la República Argentina.

Respecto de las transacciones electrónicas transfronterizas, Argentina está considerando su adhesión a la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales de la CNUDMI y ha suscrito la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías del 11 de abril de 1980 y los Tratados de Derecho Civil Internacional (Tratados de Montevideo de 1889 y 1949) que determinan la ley aplicable a los contratos internacionales.

El nuevo Código Civil y Comercial de la Nación regula diversos aspectos del comercio electrónico en su Libro Tercero sobre los derechos personales, las obligaciones y los contratos, particularmente en el "Título III. Contratos de consumo" que, en las modalidades especiales de los contratos, regula los contratos a distancia, incluso los que se conciertan a través de medios electrónicos. Asimismo, establece que siempre que en dicho Código o en leyes especiales se exija que el contrato deba constar por escrito, este requisito se entenderá por satisfecho si el contrato con el consumidor o usuario contiene un soporte electrónico u otra tecnología similar.

De igual forma, reconoce en distintos artículos el uso de "medios o mecanismos electrónicos" para distintos hechos y/o actos jurídicos, reconociéndose así el uso de las tecnologías de la información y las comunicaciones. Con respecto a la firma digital, el Código establece que, en los instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho si se utiliza una firma digital que asegure indubitadamente la autoría e integridad del instrumento.

#### b) Protección al consumidor

La Ley N° 24.240 establece requisitos especiales para los contratos con los consumidores, a quienes les confiere el derecho de retiro sin responsabilidad alguna dentro de los cinco días siguientes a la entrega de la cosa o a la celebración del contrato, si adquirió

los bienes a través de medios electrónicos. Adicionalmente, es importante destacar los instrumentos de autorregulación que diversos sectores de la industria han incorporado para proteger los derechos de los consumidores, entre los cuales destacan el Código de Conducta de la Cámara de Empresas de Información Comercial y el Código de Ética de la Asociación de Marketing Directo e Interactivo de Argentina.

A nivel regional, es preciso señalar que Argentina ha integrado en su derecho interno la Resolución Grupo Mercado Común (GMC) MERCOSUR N° 21/2004, Derecho a la Información del Consumidor en las Transacciones Comerciales efectuadas a través de Internet.

En el ámbito provincial, destaca la Ley N° 2.244 de la Ciudad Autónoma de Buenos Aires, que obliga a las personas que comercialicen o presten servicios a consumidores y/o usuarios vía un sitio web, en el ámbito de la Ciudad Autónoma de Buenos Aires, a que incluyan un enlace a la Dirección General de Defensa y Protección al Consumidor.

De igual forma, la Ley N° 2.817 de la Ciudad Autónoma de Buenos Aires establece distintas obligaciones para los proveedores que comercialicen bienes o servicios con los consumidores. La Ley establece, con respecto a los contratos de prestación de servicios celebrado por medios electrónicos u otros medios a distancia, que el consumidor tendrá derecho a un acceso claro, comprensible e inequívoco de las condiciones generales del mismo y a la posibilidad de almacenarlos o imprimirlos, dejándose debida constancia que el contrato podrá ser rescindido a elección del consumidor o usuario mediante el mismo medio utilizado para su celebración.

Asimismo, la Ley N° 863 de la Ciudad Autónoma de Buenos Aires establece que los establecimientos comerciales que brinden acceso a Internet deben instalar y activar filtros de contenido sobre páginas pornográficas. Por su parte, la Ley N° 26.104, Publicidad con Fines Turísticos, establece que toda publicidad contenida en medios electrónicos cuyas imágenes exhiban atractivos turísticos, debe cumplir con diversos requisitos de información.

Cabe señalar que, en virtud del nuevo Código Civil y Comercial de la Nación, se regulan los Contratos de consumo y, entre otros derechos, se incorpora el derecho de retracto sin responsabilidad para el consumidor, siempre que se lleve a cabo dentro de los diez días posteriores a la aceptación de la oferta.

#### c) Protección de datos personales

En materia de protección de datos personales, la Ley N° 25.326 ha incorporado un régimen de protección

acorde con la normativa europea, la Directiva 95/46/CE. En virtud de esa Ley, se ha establecido la Dirección Nacional de Protección de Datos Personales, organismo de control ad hoc que se encarga de vigilar el cumplimiento de la ley en los distintos ámbitos. En 2003, la Unión Europea reconoció que la normativa Argentina cumplía con la regulación del Consejo de Europa. Es preciso mencionar que, en virtud del Decreto N° 1.558/2001, se reglamenta la Ley de Protección de los Datos Personales.

#### d) Propiedad industrial e intelectual

Por su parte, en el ámbito de la propiedad intelectual, Argentina ha suscrito:

- los Tratados de la OMPI sobre Derecho de Autor (WCT) y sobre Interpretación o Ejecución y Fonogramas (WPPT);
- el Convenio de Berna para la Protección de las Obras Literarias y Artísticas;
- el Convenio de Ginebra para la protección de los productores de fonogramas contra la reproducción no autorizada de sus fonogramas;
- la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma);
- el Convenio de Bruselas sobre la distribución de señales portadoras de programas transmitidas por satélite, y
- el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), administrado por la Organización Mundial del Comercio (OMC).

#### e) Nombres de dominio

Con relación a los nombres de dominio, es importante señalar que, a solicitud de la Cancillería, el Colegio Público de Abogados de la Capital Federal (CPACF) elaboró un Reglamento de Arbitraje para nombres de dominio y se propuso que dicho Colegio fuese la instancia a cargo de resolver las controversias relacionadas con los nombres de dominio en Argentina, entre ellas, las relacionadas con los casos de ciberocupación. Adicionalmente y, en virtud de la Resolución N° 20/2014, la plataforma NIC.ar dejó de ser administrada por la Cancillería para entrar en el ámbito de atribuciones de la Secretaría Legal y Técnica de la Presidencia.

Desde febrero de 2014, el registro de los nombres de dominio dejó de ser gratuito y debe abonarse un im-

porte de 160 pesos argentinos para llevar a cabo el proceso de alta.

#### f) Delitos informáticos y Seguridad de la información

En el ámbito penal, la Ley N° 26.388, del 24 de junio de 2008, modificatoria del Código Penal, tipifica algunos delitos informáticos tales como la interceptación de comunicaciones, el acceso ilícito a los sistemas de cómputo, el daño informático, el fraude, la falsificación de documentos electrónicos o informáticos, la interrupción de comunicaciones y la supresión o alteración de pruebas digitales. De igual forma, mediante otras disposiciones, como las de la Ley N° 25.036, se castiga la violación de los derechos de propiedad intelectual vinculados con el software y, mediante la Ley N° 25.506, se castiga el delito de falsificación de firma digital. La Ley de Inteligencia Nacional tipifica el delito de violación de secretos e interceptación indebida de las comunicaciones.

En materia de seguridad de la información, mediante la Resolución 580/2011 de la Jefatura de Gabinete de Ministros, fechada el 28 de julio de 2011, se creó el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad en el marco de la Oficina Nacional de Tecnologías de Información (ONTI) y, mediante la Disposición 3/2013 de la ONTI, de fecha 27 de agosto de 2013, se aprobó la “Política de Seguridad de la Información Modelo” para el Sector Público Nacional, la cual incluye además la operación de un CERT nacional.

A nivel nacional, se creó el Comando de Ciberdefensa por Resolución del Ministerio de Defensa N° 343, de fecha 14 de mayo de 2014. A nivel regional, en 2014 se crearon diversas iniciativas desde UNASUR para establecer una política de ciberdefensa conjunta.

En el ámbito internacional, Argentina ha adoptado la Declaración “Fortalecimiento de la Seguridad Cibernética en las Américas” y la Declaración de Panamá sobre “La Protección de la Infraestructura Crítica en el Hemisferio frente al Terrorismo” del CICTE de la OEA. Cabe señalar que Argentina forma parte de la COM-JIB.

#### g) Iniciativas de Ley y retos

En el marco de las iniciativas de Ley que se encuentran en proceso de debate parlamentario figura el Anteproyecto de Ley Formato Digital de los Actos Jurídicos - Comercio Electrónico, el cual se presentó al Congreso en agosto de 2000. Asimismo, en el Congreso se encuentra en proceso de discusión el proyecto de Ley – Comercio por Internet, Derogación de las Resoluciones 3579/2014 y 3582/2014 de la Administración Federal de Ingresos Públicos (AFIP).

Entre los principales retos que enfrenta Argentina se encuentra lograr que las provincias se adhieran a la Ley N° 25.506 y, en el contexto internacional, la adhesión de Argentina al Convenio del Consejo de Europa sobre la Ciberdelincuencia y la suscripción a la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales de la CNUDMI.

## BOLIVIA

La Constitución Política del Estado Plurinacional de Bolivia del 9 de febrero de 2009 reconoce como derechos fundamentales el derecho a la comunicación, el derecho a la información y el derecho a la libertad de expresión, que encuentran en las nuevas tecnologías de información y comunicación un medio que permite su implementación y la incorporación del conocimiento a la sociedad.

### a) Transacciones electrónicas/ Firmas electrónicas

En Bolivia, el comercio electrónico se regula en el Capítulo Cuarto, Comercio Electrónico, del Título IV. Desarrollo de contenidos y Aplicaciones de tecnologías de información y comunicación de la Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación (Ley N° 164, 8 de agosto de 2011) sobre la oferta de bienes y servicios, validez de los contratos electrónicos, valoración y controversias.

La Ley N° 164 otorga el valor jurídico probatorio al acto o negocio jurídico realizado por persona natural o jurídica en documento digital y aprobado por las partes a través de firma digital; al mensaje electrónico de datos, y a la firma digital, y regula el correo electrónico personal, laboral y las comunicaciones publicitarias por medios electrónicos. Los documentos digitales carentes de firma digital serán admisibles como principio de prueba o indicios.

Por su parte, el Decreto Supremo N° 1793 - Reglamento a la Ley N° 164 de Desarrollo de Tecnologías de Información y Comunicación, de fecha 13 de noviembre de 2013, desarrolla con mayor detalle los requerimientos técnicos, administrativos y legales de la firma electrónica, la firma digital, el certificado digital, la Entidad Certificadora Raíz, la Entidad Certificadora y la Autoridad de Registro.

La Ley N° 393 de Servicios Financieros, de fecha 21 de agosto de 2013, también faculta a las instituciones financieras para prestar sus servicios a través de medios electrónicos, los que necesariamente deben cumplir las medidas de seguridad que garanticen la integridad, confidencialidad, autenticación y no repudio. Tales operaciones y la información contenida

y transmitida como mensajes electrónicos de datos tendrán los mismos efectos legales, con validez probatoria suficiente como un documento escrito con firma autógrafa

La Autoridad de Supervisión del Sistema Financiero (ASFI) y el Banco Central de Bolivia (BCB), de acuerdo con sus competencias, tienen la facultad de promulgar leyes que establezcan el procedimiento y la normativa de seguridad para las operaciones, así como los requisitos mínimos que deben cumplir las entidades para realizar actividades de banca electrónica, banca por teléfono y mediante dispositivos móviles, normativa de cumplimiento obligatorio por parte de las entidades financieras que p esten el servicio.

En cuanto a las leyes fiscales, el Código Tributario (Ley N° 2492), del 2 de agosto de 2003, establece como medios legales de prueba los medios informáticos y las impresiones de la información contenida en ellos, conforme con la reglamentación que al efecto se dicte. La facturación, la presentación de declaraciones juradas y de toda otra información de importancia fiscal, la retención, la percepción y el pago de tributos, el llevado de libros, los registros y anotaciones contables así como la documentación de las obligaciones tributarias y la conservación de dicha documentación, siempre que sean autorizados por la Administración Tributaria a los sujetos pasivos y terceros responsables, así como las comunicaciones y notificaciones que aquella realice a estos últimos, podrán efectuarse por cualquier medio electrónico.

La Resolución Normativa de Directorio N° 10-0049-13 - Sistema de Facturación Virtual, de fecha 30 de diciembre de 2013, establece que en el marco del Modelo de Administración del Sistema Impositivo (MASI) se ha desarrollado el Sistema de Facturación Virtual (SFV). El SFV hace uso intensivo de Internet para la modernización, optimización e integración de procesos y aplicaciones impositivas, con la premisa de dotar al Servicio de Impuestos Nacionales de mecanismos de control oportunos y eficientes que le permitan cumplir adecuadamente con sus fines y facilitar el cumplimiento de las obligaciones tributarias de los sujetos pasivos o terceros responsables. Las operaciones electrónicas realizadas y registradas en el sistema computarizado de la Administración Tributaria por un usuario autorizado surten efectos jurídicos.

La Resolución Normativa de Directorio N° 10-0044-13, de fecha 20 de diciembre de 2013, del Servicio de Impuestos Nacionales tiene por objeto reglamentar aspectos tributarios en la venta de bienes a través del comercio electrónico dentro del territorio nacional. Alcanza a las operaciones de venta de bienes mediante

comercio electrónico que sean realizadas por las personas naturales o jurídicas.

#### b) Protección al consumidor

Además de la tutela constitucional que mediante los artículos 75 y 76 se confiere a los consumidores en términos generales, la Ley General de los derechos de las usuarias y los usuarios y de las consumidoras y los consumidores (Ley N° 453), de fecha 4 de diciembre de 2013, no establece de forma específica los productos o servicios prestados por medios electrónicos, sin embargo, se puede considerar que los mismos se incluyen en el ámbito de aplicación. La Ley regula el derecho a la información, la publicidad e información engañosa o abusiva. También obliga al cumplimiento de las condiciones ofertadas, regula el contenido de los contratos de adhesión y prohíbe las cláusulas abusivas. Asimismo, regula el derecho a la reclamación, el otorgamiento de garantías en los servicios, los deberes de las usuarias y los usuarios y de las consumidoras y los consumidores, los deberes de los proveedores, así como las reglas para procesar las reclamaciones administrativas y las formas de restauración, entre otras disposiciones.

#### c) Protección de datos personales

En relación a la protección de datos personales, la Constitución Política del Estado Plurinacional de Bolivia establece la Acción de Protección de Privacidad, que reconoce la facultad que tiene el titular del dato, la persona moral o colectiva para exigir el derecho a conocer, objetar, cancelar o eliminar sus datos personales. Asimismo, reconoce el derecho fundamental a la intimidad o privacidad personal o familiar, o a su propia imagen, honra y reputación. En el Código Procesal Constitucional del 5 de julio de 2012 se establece, en el Capítulo Cuarto Acción de Protección de Privacidad, el procedimiento para interponer la acción de protección de privacidad, sin necesidad de reclamo administrativo previo por la inminencia de la violación del derecho tutelado, y la acción tiene un sentido eminentemente cautelar.

Por su parte, el Decreto Supremo Reglamentario de la Ley N° 164 de Telecomunicaciones, Tecnologías de Información y Comunicación establece algunos lineamientos para el tratamiento de los datos personales. Entre las principales medidas se encuentra el consentimiento expreso del titular. De igual forma, señala que las personas a las que se les solicite datos personales deberán ser previamente informadas de que sus datos serán objeto de tratamiento, de la finalidad de la recolección y el registro de estos, de los potenciales destinatarios de la información, de la identidad y el domicilio del responsable del tratamiento o

de su representante, y de la posibilidad de ejercitar los derechos de acceso, rectificación, actualización, cancelación, objeción, revocación y otros que fueren pertinentes.

Asimismo, el Código Tributario (Ley N° 2492), del 2 de agosto de 2003, establece que las declaraciones y los datos individuales obtenidos por la Administración Tributaria tendrán carácter reservado. Solo podrán ser utilizados para la efectiva aplicación de los tributos o procedimientos cuya gestión tenga encomendada, y no podrán ser informados, cedidos o comunicados a terceros, salvo que medie orden judicial debidamente fundamentada, o una solicitud de información de conformidad con lo establecido por el Artículo 70 de la Constitución. La información agregada o estadística general es pública.

Adicionalmente, la Ley de Servicios Financieros (Ley N° 393) dispone que toda persona individual o colectiva que considere estar indebidamente o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por las entidades financieras, por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad o privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de la Privacidad prevista en la Constitución.

#### d) Propiedad Industrial e Intelectual

En el ámbito de la propiedad intelectual, Bolivia ha incorporado en su Ley de Derecho de Autor (Ley N° 1322), de fecha 13 de abril de 1992, la protección a los programas de computadora (software) y ha emitido el Decreto Supremo N° 24582 - Reglamento del Soporte Lógico o Software, de fecha 25 de abril de 1997. De igual forma, mediante Decreto Supremo N° 0667 - Texto Ordenado del Código Penal, de fecha 8 de octubre de 2010, se tipifican los delitos contra la propiedad intelectual vinculados con la reproducción, plagio, distribución, publicación, transformación y comercialización a gran escala de obras protegidas por derechos de autor, sin la correspondiente autorización de su titular.

Por su parte, en el ámbito internacional de la propiedad intelectual, Bolivia ha suscrito:

- los Tratados de la OMPI sobre Derecho de Autor (WCT) y sobre Interpretación o Ejecución y Fonogramas (WPPT);
- el Convenio de Berna para la Protección de las Obras Literarias y Artísticas, la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogra-

mas y los organismos de radiodifusión (Convención de Roma), y

- el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), administrado por la Organización Mundial del Comercio (OMC).

#### e) Nombres de dominio

En materia de nombres de dominio, el NIC Bolivia (.bo) cuenta con las Políticas de Delegación de Nombres de Dominio bajo el ccTLD.bo, la Política de solución de controversias en materia de Nombres de Dominio registrados bajo el ccTLD .bo y el Reglamento de la Política de solución de controversias, que reconoce dentro de los proveedores de servicios de arbitraje al Centro de Arbitraje y Mediación de la Organización Mundial de la Propiedad Intelectual y al Centro de Conciliación y Arbitraje Comercial de la Cámara Nacional de Comercio de Bolivia.

#### f) Delitos Informáticos y Seguridad de la Información

En materia de delitos informáticos, el Código Penal aprobado mediante la Ley N° 1768, del 10 de marzo de 1997, tipifica los delitos relacionados con la manipulación informática y alteración, acceso y uso indebido de datos informáticos. Por su parte, la Ley de Servicios Financieros (Ley N° 393) ha incluido diversos delitos relacionados con el fraude a través de medios electrónicos, entre otros, la apropiación indebida de fondos financieros.

#### g) Iniciativas de Ley y retos

Entre los principales retos que enfrenta Bolivia se encuentra el adoptar una legislación general en materia de datos personales, a efectos de cumplir con los compromisos asumidos en la Red Iberoamericana de Protección de Datos. De igual forma, precisa revisar su legislación penal sustantiva y procesal con el fin de actualizarla, teniendo en cuenta el Convenio del Consejo de Europa sobre la Ciberdelincuencia así como el Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia, la Recomendación de la COMJIB relativa a la Tipificación y Sanción de la Ciberdelincuencia, de la cual forma parte.

Bolivia también enfrenta el problema de la brecha digital, requiriéndose de políticas públicas adecuadas para promover la conectividad y las capacidades digitales.

## BRASIL

Brasil cuenta con distintos ordenamientos que rigen diversos aspectos del comercio electrónico, varios de

ellos de reciente creación, como la Ley de Comercio Electrónico por Decreto N° 7.962, así como el Marco Civil de Internet mediante la Ley N° 12.965, del 23 de abril de 2014, cuyo contenido se describe a continuación.

#### a) Transacciones electrónicas / Firmas electrónicas

La Ley de Comercio Electrónico, mediante Decreto N° 7.962, del 15 de marzo de 2013, establece diversas obligaciones para quienes comercializan productos y servicios en línea, centrándose en temas de protección al consumidor que se analizan en el apartado siguiente.

En virtud de la Medida Provisional 2200-2, del 24 de agosto de 2001, emitida por la Presidencia de la República, se crea la Infraestructura de Claves Públicas de Brasil (ICP-Brasil), con el objetivo de garantizar la autenticidad, integridad y validez jurídica de los documentos electrónicos, aplicaciones y soporte de aplicaciones utilizando certificados digitales y la realización de transacciones electrónicas seguras. Se otorgan facultades a la ICP-Brasil para formular políticas con miras a gestionar tanto a las autoridades de certificación (AC) como a las autoridades de registro (AR). También se otorgan facultades al Instituto Nacional de Tecnología de la Información (ITI), dependiente del Ministerio de Ciencia, Tecnología e Innovación, para desempeñar las funciones de Autoridad Certificadora Raíz de la Infraestructura de Claves Públicas en Brasil y para llevar a cabo actividades de supervisión, así como para sancionar a quienes infrinjan el marco normativo.

La Medida Provisional confiere a los documentos electrónicos, públicos o privados, producidos bajo el proceso de certificación de la ICP-Brasil, todos los efectos legales. Asimismo, permite el uso de documentos electrónicos para efectos fiscales, siempre que cumplan con los requisitos del Código Fiscal de la Nación. La ICP-Brasil cuenta con facultades para negociar y aprobar acuerdos bilaterales de certificación, acuerdos de certificación cruzada, interoperabilidad y otras formas de cooperación internacional.

Por otra parte, la Ley N° 12.682, del 9 de julio de 2012, confiere valor legal a la digitalización, al almacenamiento en medios electrónicos y a la reproducción de documentos públicos y privados electrónicos, ópticos o equivalentes, así como a los medios para explorar la conversión de la representación de un documento de código digital. El proceso de exploración se debe realizar con el fin de mantener la integridad, autenticidad y, de ser necesario, la confidencialidad de los documentos digitales, y se debe usar el certificado digital emitido en el marco de la ICP-Brasil. Asimismo, señala que los medios de comunicación de

documentos digitales de almacenamiento deben protegerse del acceso, uso, modificación, reproducción y destrucción no autorizada.

En el ámbito gubernamental, el Marco Civil de Internet establece que los aplicativos de Internet de los entes del Poder Público deben procurar: i) la compatibilidad de los servicios de gobierno electrónico con diferentes terminales, sistemas operativos y aplicaciones de acceso, así como su interoperabilidad entre los diferentes niveles federativos y diferentes sectores de la sociedad, y ii) la facilidad de uso de los servicios de gobierno electrónico. Asimismo, promueve la adopción preferencial de tecnologías, estándares y formatos abiertos y libres, igual que la publicidad y difusión de los datos y la información pública, de forma abierta y estructurada.

Adicionalmente, Brasil ha suscrito las dos resoluciones del MERCOSUR respecto de los estándares sobre el uso de firmas digitales, a saber, la Resolución N° 34/06 y la Resolución N° 37/06 relativas a la firma electrónica y la firma digital

#### b) Protección al consumidor

La Ley N° 8.078, del 11 de septiembre de 1990, o Código de Defensa del Consumidor es el ordenamiento de mayor relevancia en la materia. Establece que los proveedores no pueden condicionar la ejecución de los contratos con los consumidores sujetándola a la aceptación del almacenamiento o divulgación de su información; cualquier cláusula en este sentido es considerada inválida y nula y puede ser sancionada por las autoridades en materia de competencia económica. Cabe señalar que, además de la responsabilidad civil que los proveedores pueden enfrentar por incumplir el Código, también pueden enfrentar procesos penales si se acredita alguno de los delitos previstos en este Código, a saber: i) obstaculizar u obstruir el acceso a los consumidores a información referente a su persona que conste en archivos, bases de datos, formatos o registros, que se sanciona con pena de seis meses a un año de cárcel o con multa, y ii) no corregir de inmediato la información de los consumidores incluida en archivos, bases de datos, formatos o registros que el proveedor tenga conocimiento o debiera tenerlo sobre la inexactitud, la cual se sanciona con pena de uno a seis meses de prisión o con multa.

Por otra parte, la Ley de Comercio Electrónico (Decreto N° 7.962), del 15 de marzo de 2013, establece diversas obligaciones a los proveedores, como el deber de suministrar información sobre los productos, incluyendo la descripción completa de sus características, las condiciones de la contratación así como

los beneficios y ventajas del producto, datos técnicos, advertencias o instrucciones de uso, las opciones disponibles, las garantías y condiciones de devolución o cambio. También obliga a proporcionar la información de contacto del proveedor, como el número telefónico, el correo electrónico o un enlace al formulario con datos para establecer contacto, la dirección física de la empresa y el proceso para el retorno del producto sin responsabilidad para el comprador.

Asimismo, obliga a brindar información sobre el producto, entre otros, el precio, la disponibilidad, las formas y modalidades de pago y las opciones de entrega. Previo a la conclusión de la contratación y a la aplicación y el registro del pago, se debe dar acceso al comprador al contrato que deberá aceptar, así como a un mecanismo para modificar errores o datos incorrectos. El contrato de venta debe incluir los términos de aceptación así como las condiciones para ejercer el derecho de retracto sin penalizaciones.

Por su parte, el Marco Civil de Internet vela por la aplicación de las normas de protección y defensa del consumidor en las relaciones de consumo realizadas en Internet y señala que son nulas todas las cláusulas que la contravengan, al igual que aquellas que impliquen una ofensa a la inviolabilidad y al secreto de las comunicaciones privadas a través de Internet o que, en la contratación, no ofrezcan al contratante la adhesión al foro (jurisdicción) brasileño para la solución de conflictos derivados de servicios prestados en Brasil. También promueve el uso de herramientas de control parental para la protección a menores, así como la instrumentación de medidas y procedimientos de seguridad que permitan conservar la confidencialidad de la información y que deben ser informados por el responsable de la provisión de servicios de forma clara. Considera, asimismo, medios de defensa individuales y colectivos. Además defiende el principio de neutralidad de la red, que prohíbe en el suministro de la conexión a Internet (de pago o gratuita), así como en la transmisión, conmutación o enrutamiento, el bloquear, monitorear, filtrar o analizar el contenido de los paquetes de datos. Asimismo, dispone que las actividades que sean llevadas a cabo por personas jurídicas domiciliadas en el exterior, que ofrezcan servicios al público brasileño, o que cuenten con al menos un integrante del mismo grupo económico que tenga establecimiento en Brasil, responden solidariamente por los incumplimientos de sus filiales, sucursales, oficinas o establecimientos situados en Brasil.

#### c) Protección de datos personales

Brasil forma parte del MERCOSUR así como de la Red Iberoamericana de Protección de Datos. Consagra en

su Constitución Federal el derecho a la intimidad, a la vida privada, al honor y a la imagen de las personas, y asegura el derecho a ser indemnizado por el daño material o moral que se derive de su violación. De igual forma, reconoce la inviolabilidad del secreto de la correspondencia, de las comunicaciones telegráficas, de las informaciones y de las comunicaciones telefónicas, salvo, en el último caso, que exista una orden judicial para fines de investigación criminal o instrucción penal. También consagra la acción de *habeas data*, que se traduce en el derecho a conocer la información que sobre los datos personales tengan las instancias del sector público, así como el derecho de rectificación.

Brasil no cuenta con una Ley general de protección de datos personales, sin embargo, en distintas leyes protege el derecho a la vida privada de los individuos. Entre esas leyes, se encuentra la Ley N° 10.406/2002 del Código Civil, fechado el 10 de enero de 2002, que reconoce la inviolabilidad de la privacidad de las personas, al igual que el Código de Defensa del Consumidor (CDC) que contiene diversas reglas relativas al acceso a las bases de datos o expedientes de los consumidores, así como a su almacenamiento y mantenimiento. El CDC señala que la disponibilidad de los datos de los consumidores debe sustentarse en una solicitud individual centrada en un consumidor concreto, pues el Código prohíbe el suministro de información masivo sobre múltiples personas. También debe provenir de una relación comercial específica, de un posible acuerdo entre el consumidor y el proveedor que la solicita.

El Marco Civil de Internet tutela los siguientes derechos de los usuarios: i) la inviolabilidad de la intimidad y de la vida privada, asegurando el derecho a su protección y a la indemnización por el daño material o moral resultante de su violación; ii) la inviolabilidad del flujo y secreto de las comunicaciones por Internet, salvo por orden judicial, así como la inviolabilidad y el secreto de las comunicaciones privadas almacenadas, salvo por orden judicial; iii) la no suspensión de la conexión a Internet, salvo deuda contraída directamente por su utilización; iv) la información clara y completa en los contratos de prestación de servicios, detallando el régimen de protección de datos de los registros de conexión y de los registros de acceso a aplicaciones en Internet; v) la imposibilidad de suministrar a terceros datos personales de los usuarios, incluyendo registros de conexión y acceso a aplicaciones en Internet, salvo que medie consentimiento libre, expreso e informado o en circunstancias establecidas por la ley; vi) información clara y completa sobre la recolección, uso, almacenamiento, tratamiento y pro-

tección de los datos personales de los usuarios, que solo podrán ser utilizados para finalidades que justifiquen su recolección, sean legales y especificadas en los contratos de prestación de servicios; vii) que el consentimiento expreso sobre la recolección, uso, almacenamiento y tratamiento de datos personales, se presente de forma destacada de las demás cláusulas contractuales, y viii) el borrado definitivo de los datos personales con las salvedades de ley.

También establece que en cualquier operación de recolección, almacenamiento, protección o tratamiento de registros, datos personales o de comunicaciones por proveedores de conexión y de aplicaciones de Internet, en las que por lo menos uno de estos actos ocurra en territorio nacional, se deberá cumplir la legislación brasileña, así como con los derechos a la privacidad y a la protección de los datos personales y el secreto de las comunicaciones privadas y de los registros.

#### d) Propiedad Industrial e Intelectual

La Ley de Software (Ley N° 9.609), del 19 de febrero de 1998, establece las reglas para proteger a los programas de ordenador como obras protegidas bajo el régimen del derecho de autor y establece, entre otras cuestiones, las condiciones para su comercialización en Brasil. También establece las garantías que el titular de los derechos de autor debe dar a los usuarios del programa informático, así como las sanciones aplicables en caso de infringir la ley.

Por su parte, en el ámbito internacional de la propiedad intelectual, Brasil ha suscrito:

- los Tratados de la OMPI sobre Derecho de Autor (WCT) y sobre Interpretación o Ejecución y Fonogramas (WPPT);
- el Convenio de Berna para la Protección de las Obras Literarias y Artísticas;
- el Convenio de Ginebra para la protección de los productores de fonogramas contra la reproducción no autorizada de sus fonogramas;
- la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma), y
- el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), administrado por la Organización Mundial del Comercio (OMC).

#### e) Nombres de dominio

Por lo que respecta a los nombres de dominio-país .br correspondiente a Brasil, compete al Centro de Información de la Red Brasileña (NIC.br), brazo ejecu-

tivo del Comité Gestor de Internet (CGI.br), el registro y mantenimiento de los nombres de dominio .br, así como la asignación de Números de Sistemas Autónomos (ASN) y las direcciones IPv4 o IPv6 en el país, bajo la coordinación del Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC).

El NIC.br cuenta con un Sistema Administrativo de Internet para el Conflicto de nombres de dominio (SA-CI-Adm), cuyo Reglamento establece las reglas para la solución de controversias entre el titular del nombre de dominio y cualquier tercero que impugne la legitimidad del registro de un nombre de dominio y que reconoce como prestadores del servicio de arbitraje a la Asociación Brasileña de Propiedad Intelectual (Associação Brasileira da Propriedade Intelectual (ABPI)), a la Cámara de Comercio Brasil-Canadá (Câmara de Comércio Brasil-Canadá (CCBC)) y a la Organización Mundial de la Propiedad Intelectual.

#### f) Delitos Informáticos y Seguridad de la Información

En el ámbito de los delitos informáticos, la Ley N° 12.735 y la Ley N° 12.737, ambas del 30 de noviembre de 2012, tipifican diversas conductas realizadas mediante el uso de aparatos electrónicos, digitales o similares, contra sistemas informáticos y otros afines, modificando el Código Penal del Brasil.

En virtud de la Ley N° 12.737, se incluye el delito de “invasión a un dispositivo informático” a efectos de sancionar a quien invada un dispositivo informático, conectado o no a la red informática, mediante la violación indebida de un mecanismo de seguridad, con el fin de obtener, manipular o destruir datos o información, sin la autorización expresa o tácita del titular del dispositivo, o de instalar vulnerabilidades para obtener una ventaja ilícita.

Asimismo, sanciona a quien produzca, ofrezca, distribuya, venda o difunda dispositivos o programas de ordenador, con el fin de permitir las conductas precitadas. Las penas se amplían si la invasión resulta en una pérdida económica. También castiga a quien reciba secretos comerciales e industriales o contenido privado en razón de la violación del mecanismo de seguridad del equipo de cómputo. Se consideran agravantes si los delitos antes referidos se cometen contra los funcionarios públicos, incluido el presidente, gobernadores y otros funcionarios del nivel federal, estatal o municipal.

En lo referente a la seguridad de la información, el Marco Civil de Internet tutela la garantía de neutralidad de la red así como la preservación de la estabilidad, seguridad y funcionalidad de la misma. En la provisión del servicio de conectividad a Internet, el adminis-

trador del sistema debe mantener los registros de conexión por un año, en un ambiente controlado, seguro y de confidencialidad. Se faculta a la autoridad policial o administrativa o al Ministerio Público para requerir cautelarmente que los registros guardados se conserven por más tiempo. El proveedor de aplicaciones de Internet también debe mantener los respectivos registros de acceso a aplicaciones de Internet, por seis meses, en un ambiente controlado, seguro y de confidencialidad. La autoridad policial o administrativa o el Ministerio Público puede solicitar cautelarmente que los registros de acceso a las aplicaciones de Internet se conserven por más tiempo.

Cabe señalar que el proveedor de conexión a Internet no será responsabilizado civilmente por los daños surgidos por el contenido generado por terceros. Por su parte, el proveedor de aplicaciones de Internet solamente podrá ser responsabilizado por daños que surjan del contenido generado por terceros si, después de una orden judicial específica no toma las previsiones, en el ámbito de los límites técnicos de su servicio y dentro del plazo asignado, para poner a disposición el contenido especificado como infractor.

#### g) Iniciativas de Ley y retos

Entre las iniciativas de Ley más relevantes que se encuentran en proceso de debate parlamentario figura el proyecto de Ley General de Protección Datos de 2011, así como diversas reformas a la legislación procesal penal para alinearla con el Convenio del Consejo de Europa sobre la Ciberdelincuencia. La reducción de la brecha digital, particularmente en torno a la ausencia de capacidades en materia de tecnología de la información, constituye uno de los principales retos para Brasil.

## CHILE

La legislación en materia de comercio electrónico de Chile se encuentra en distintos ordenamientos, entre los cuales destaca la Ley sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma (Ley N° 19.799), fechada el 25 de marzo de 2002, así como la Ley N° 20.217, que modifica la primera ley y el Código de Procedimiento Civil, fechada el 12 de noviembre de 2007. Asimismo, destaca la Ley sobre Protección de los Derechos de los Consumidores (Ley N° 19.496), fechada el 7 de marzo de 1997 y la Ley de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios (Ley N° 19.886), fechada el 30 de julio de 2003, cuyo contenido se revisa en los apartados siguientes.

#### a) Transacciones electrónicas / Firmas electrónicas

La Ley N° 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma (2002) de Chile se basa en diversas disposiciones de la Ley Modelo de la CNUDMI sobre Firmas Electrónicas, así como en la Ley del Estado de Utah sobre la Firma Digital<sup>25</sup>. La Ley N° 19.799 establece que los actos y contratos otorgados o celebrados por personas naturales o jurídicas, públicas o privadas, suscritos por medio de firma electrónica, serán válidos de la misma manera y producirán los mismos efectos que los celebrados por escrito y en soporte de papel. Dichos actos y contratos se reputarán como escritos, en los casos en que la ley exija que los mismos consten por escrito.

La Ley N° 19.799 faculta a los órganos del Estado para ejecutar o realizar actos, celebrar contratos y expedir cualquier documento, dentro de su ámbito de competencia, suscribiéndolos con firma electrónica. También establece las obligaciones de los prestadores de servicios de certificación, así como los requisitos de los certificados de firma electrónica y los derechos y obligaciones de los usuarios de las firmas electrónicas.

Mediante Decreto 181 de la Ley N° 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma, fechado el 17 de agosto de 2002, se regulan con mayor detalle el actuar de los prestadores de servicios de certificación, su proceso de certificación, así como la protección de los derechos de los usuarios y la utilización de la firma electrónica por los órganos de la Administración del Estado. También se establecen las normas técnicas relativas a los certificados digitales, el sellado de tiempo y los servicios de firma móvil

Por su parte, la Ley N° 20.217 que modifica el Código de Procedimiento Civil, y la Ley N° 19.799 sobre Documentos Electrónicos, Firma Electrónica y los Servicios de Certificación de dicha Firma incorporan en el primer ordenamiento la inclusión de una prueba complementaria de autenticidad para documentos electrónicos no suscritos con firma electrónica avanzada y, en el segundo ordenamiento, se introduce el concepto de fecha electrónica.

Adicionalmente, la Ley de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios (Ley N° 19.886) establece que los organismos públicos deben cotizar, licitar, contratar, adjudicar, solicitar el despacho y, en general, desarrollar todos sus procesos de adquisición y contratación de bienes, a través de sistemas electrónicos autorizados

por la Dirección de Compras y Contratación Pública, sea a través de redes abiertas o cerradas, utilizando plataformas de comercio electrónico o mercados digitales de transacciones. De igual forma, establece un registro electrónico oficial en el que se deben inscribir todas las personas naturales y jurídicas, chilenas y extranjeras habilitadas que contraten con los organismos del Estado. Los organismos públicos no pueden, como regla general, adjudicar contratos cuyas ofertas no hayan sido recibidas a través de los sistemas electrónicos o digitales.

Con el propósito de reconocer la validez tributaria de las operaciones comerciales, efectuadas mediante documentos generados electrónicamente, diversos ordenamientos han sido emitidos y/o modificados para permitir la instrumentación de la facturación electrónica en Chile. Entre los ordenamientos más relevantes se encuentran: i) el Decreto Ley N° 825 sobre Impuesto a las Ventas y Servicios, fechado el 31 de diciembre de 1974; ii) la Resolución Exenta N° 09 del Servicio de Impuestos Internos (SII), fechada el 15 de febrero de 2001, que a instancias del Código Tributario establece diversas normas que regulan el uso de firmas y certificados electrónicos en materia tributaria; iii) la Ley N° 19.983 que regula la transferencia y otorga mérito ejecutivo a la copia de la factura, fechada el 15 de diciembre de 2004; iv) la Resolución Exenta SII N° 86, fechada el 1 de septiembre de 2005, que establece las normas y procedimientos para que los contribuyentes autorizados emitan facturas electrónicas, y v) el Decreto Ley N° 830 sobre Código Tributario, fechado el 31 de diciembre de 1974 y actualizado hasta el 28 de mayo de 2014, que autoriza que los documentos se archiven en medios distintos al papel.

Por su parte, destaca también la automatización de diversos procesos aduanales del Servicio Nacional de Aduanas, para agilizar el despacho aduanero, mediante el envío de información a través de medios remotos y su correspondiente validación en diversas bases de datos. La participación de Chile en el APEC, la OMC y la Organización Mundial de Aduanas (OMA) ha impulsado la modernización de sus Aduanas. Entre los cuerpos normativos más relevantes en materia aduanera se encuentra la Ley N° 19.479, que introduce modificaciones a la Ordenanza de Aduanas y a la Ley Orgánica del Servicio Nacional de Aduanas, fechada el 21 de noviembre de 1996, la cual dicta normas sobre la gestión y el personal, así como el Decreto con Fuerza de Ley N° 30, fechado el 4 de junio de 2005, por virtud del cual el Servicio Nacional de Aduanas implementa un sistema de pago electrónico

<sup>25</sup> Estado perteneciente a los Estados Unidos de Norteamérica.

de derechos, impuestos, tasas y demás gravámenes que perciben las Aduanas.

#### b) Protección al consumidor

En materia de comercio electrónico, la Ley sobre Protección de los Derechos de los Consumidores (Ley N° 19.496) obliga a los proveedores a indicar su dirección de correo postal o electrónico y los medios técnicos que pone a disposición del consumidor para identificar y corregir errores en el envío o en sus datos. De igual forma, establece que toda comunicación promocional o publicitaria enviada por correo electrónico deberá indicar la materia o asunto sobre el que versa, la identidad del remitente y contener una dirección válida a la que el destinatario pueda solicitar la suspensión de los envíos, que quedarán desde entonces prohibidos.

#### c) Protección de datos personales

Chile reconoce en su Constitución Política el derecho a la vida privada y a la honra de la persona y su familia. También consagra el derecho a la inviolabilidad de toda forma de comunicación privada y prohíbe la interceptación, apertura o registro de las comunicaciones, salvo en los casos expresamente previstos en la ley. Además de la protección constitucional, cuenta con distintas leyes que tutelan la vida privada de las personas, dentro de las cuales destaca la Ley sobre protección de la vida privada (Ley N° 19.628), de fecha 28 de agosto de 1999, modificada por la Ley N° 19.812, fechada el 13 de junio de 2002, que regula el tratamiento de los datos de carácter personal en registros o bancos de datos por parte de organismos públicos o por particulares.

La Ley protege a las personas físicas titulares de los datos personales que son objeto de tratamiento, el cual se entiende como cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar, ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma. Reconoce el derecho de las personas a la información, modificación, cancelación o bloqueo de sus datos personales, así como los medios judiciales para ejercerlos y que involucran procedimientos sumarios.

Asimismo, protege los datos de carácter personal o datos personales, entendidos como los relativos a cualquier información concerniente a personas naturales, identificadas o identificables. Establece mayores medidas para proteger los datos personales sensibles definidos como aquellos que se refieren a las caracte-

rísticas físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual. La Ley ordena que los datos sensibles no pueden ser objeto de tratamiento, a menos que la ley lo autorice, exista consentimiento del titular o se necesiten para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

La Ley consagra el derecho de las personas a la información, modificación, cancelación o bloqueo de sus datos personales, cuyos límites se encuentran en la seguridad de la Nación o el interés nacional.

La Ley señala que la persona natural o jurídica privada o el organismo público responsable del banco de datos personales deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el Tribunal, que tiene la facultad de establecer el monto de la indemnización. La Ley no designa a ninguna autoridad administrativa encargada de aplicar y hacer valer la ley, aunque sí confiere potestades al poder judicial para, en procedimiento sumario, ordenar el cumplimiento de la Ley y dictar sanciones en caso de que no se cumplan sus resoluciones.

#### d) Propiedad Industrial e Intelectual

La Ley sobre Propiedad Intelectual (Ley N° 17.336), fechada el 2 de octubre de 1970, protege a los programas computacionales y a las compilaciones de datos por toda la vida del autor y se extiende hasta por 70 años más, contados desde la fecha de su fallecimiento.

Mediante la Ley N° 20.435, que modifica la Ley sobre Propiedad Intelectual (Ley N° 17.336), fechada el 23 de abril de 2010, se incorpora por primera vez en la región el régimen de “Puerto Seguro”, limitado a los temas autorales, en el que instrumenta un procedimiento de “notificación y retiro judicial” y un apartado dedicado al procedimiento judicial sumario que se debe seguir para solicitar el retiro de materiales infractores. El procedimiento se puede dar bajo la modalidad de medidas precautorias o mediante un procedimiento judicial especial en el contexto de las medidas para limitar la responsabilidad de los prestadores de servicios de telecomunicaciones e Internet.

En virtud del modelo de “Puerto Seguro”, aquellos prestadores de servicios de telecomunicaciones e Internet que: i) no inicien la transmisión de los mate-

riales infractores; ii) no ejerzan control editorial sobre los mismos; iii) que no tengan conocimiento efectivo sobre la ilicitud de los materiales infractores, o iv) que de manera expedita retiren, bloqueen o impidan el acceso a los materiales infractores (procedimiento de notificación y retiro), no serán responsables por los materiales que transmitan, enruten, almacenen, vinculen o referencien y están exentos de la obligación de supervisar o monitorear dichos materiales, así como de la obligación de realizar búsquedas activas de hechos o circunstancias que sugieran o indiquen actividades ilícitas.

Es importante señalar que el régimen de “Puerto Seguro” de la normativa chilena cumple con la Declaración conjunta sobre Libertad de Expresión e Internet, del 1 de junio de 2011, emitida por el Relator Especial de las Naciones Unidas para la Libertad de Opinión y de Expresión, el Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Relatora Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión y la Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP).

En el Reglamento de la Ley sobre Propiedad Intelectual (Ley N° 17.336), fechado el 30 de abril de 2013, se incorporaron, entre otras disposiciones, las relacionadas con la designación del representante de los prestadores de servicios de Internet para recibir notificaciones judiciales.

En el ámbito internacional de los derechos de propiedad intelectual e industrial, Chile ha ratificado

- el Tratado de Beijing sobre Interpretaciones y Ejecuciones Audiovisuales (2012);
- los Tratados de la OMPI sobre Derecho de Autor (WCT) y sobre Interpretación o Ejecución y Fonogramas (WPPT);
- el Convenio de París para la Protección de la Propiedad Industrial (1883);
- el Convenio de Berna para la Protección de las Obras Literarias y Artísticas;
- el Convenio de Ginebra para la protección de los productores de fonogramas contra la reproducción no autorizada de sus fonogramas;
- la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma);
- el Tratado de la OMPI de Cooperación en materia de Patentes (PCT), y

- el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), administrado por la Organización Mundial del Comercio (OMC).

#### e) Nombres de dominio

El Departamento de Ciencias de la Computación de la Universidad de Chile, por delegación de la Autoridad de Números Asignados en Internet (IANA), administra el Registro de Nombres de Dominio CL, denominado NIC Chile, de acuerdo con los principios contenidos en RFC 1591: estructura y delegación del Sistema de Nombres de Dominio. Dicha delegación fue reconocida formalmente el 24 de junio de 2006 mediante un acuerdo marco suscrito entre la Corporación de Internet para la Asignación de Nombres y Números (ICANN) y NIC Chile, por el cual se establecieron las responsabilidades que ambas entidades tienen en cuanto a la preservación de la estabilidad, la seguridad y la interoperabilidad de Internet.

Los conflictos que se susciten con ocasión de la revocación de un nombre de dominio .cl serán resueltos de acuerdo con la Política de Resolución de Controversias por Nombres de Dominio.cl, y toda controversia se someterá, resolverá y tramitará de acuerdo con el procedimiento de arbitraje establecido en dicha política, que faculta al Centro de Resolución de Controversias por nombres de dominio .CL como la unidad dependiente del NIC Chile encargada de administrar el Sistema de Resolución de conflictos por nombres de dominio. El NIC Chile no tendrá ninguna participación en la etapa de arbitraje, excepto designar al árbitro de acuerdo con el procedimiento y dar cumplimiento a la resolución arbitral.

#### f) Delitos Informáticos y Seguridad de la Información

En materia penal, la Ley sobre Delincuencia Informática (Ley N° 19.223), fechada el 7 de junio de 1993, tipifica los delitos de: i) sabotaje informático, es decir, la destrucción o inutilización de un sistema de tratamiento de información o de partes o componentes, así como el impedimento, obstaculización o modificación de su funcionamiento, con agravante para el caso de que se afectaren los datos del sistema; ii) espionaje informático, consistente en interceptar, interferir, o acceder a un sistema de tratamiento de información con ánimo de apoderarse, usar o conocer indebidamente la información contenida en el mismo; iii) alteración de datos, incluida su destrucción o daño, y iv) la revelación o difusión no autorizada de datos contenidos en un sistema de tratamiento de información.

Por su parte, la Ley General de Telecomunicaciones (Ley N° 18.168), fechada el 2 de octubre de 1982,

obliga a los concesionarios y a los proveedores de acceso a Internet a procurar preservar la privacidad de los usuarios, la protección contra virus y la seguridad de la red. Adicionalmente, tipifica como delitos de acción pública: i) al que maliciosamente interfiera, intercepte o interrumpa un servicio de telecomunicaciones, a quien se le impone una pena de presidio menor en cualquiera de sus grados y el comiso de los equipos e instalaciones; ii) al que intercepte o capte maliciosamente o grave, sin la debida autorización, cualquier tipo de señal que se emita a través de un servicio público de telecomunicaciones, quien será sancionado con la pena de presidio menor en su grado medio y una multa de 50 a 5.000 unidades tributarias mensuales.

#### g) Iniciativas de ley y Retos

Entre las iniciativas de Ley, destaca el proyecto de Modificaciones a la Ley sobre Protección de la Vida Privada y Protección de Datos de Carácter Personal (Ley N° 19.628), del 11 de enero de 2012, que, entre otros, propone la supresión de las personas jurídicas como sujeto de protección y la reformulación de diversas definiciones e innovaciones al procedimiento de reclamo para facilitar su expedita tramitación, entre otras materias. La definición de una autoridad administrativa garante en materia de protección de datos constituye uno de los principales retos que deberán resolverse en la normativa de Chile.

## COLOMBIA

La normativa de Colombia reconoce en distintos ordenamientos el uso de mensajes de datos y de medios electrónicos, especialmente de firmas electrónicas, firmas digitales y certificados digitales emitidos por prestadores de servicios de certificación gubernamentales y/o privados, los cuales gozan de plena validez jurídica.

#### a) Transacciones electrónicas / Firmas electrónicas

En materia de transacciones electrónicas y firmas electrónicas, destaca la Ley N° 527 de 1999, del 18 de agosto de 1999, conocida también como “Ley de Comercio Electrónico”, la cual incorpora diversas disposiciones de las Leyes Modelo de la CNUDMI sobre Comercio Electrónico y las Firmas Electrónicas. Dicho ordenamiento autoriza el uso de mensajes de datos en el ámbito de las operaciones de comercio electrónico y contempla, entre otros aspectos, los relativos a la autenticidad, integridad, originalidad y conservación de documentos electrónicos.

De igual forma, la Ley reconoce el uso y valor probatorio de las firmas digitales amparadas por certificados

emitidos por las entidades de certificación. Esta norma ha tenido recientes reglamentaciones mediante decretos como el Decreto 2364, del 22 de noviembre de 2012, que reglamenta en Colombia la firma electrónica como un mecanismo equivalente de firma manuscrita más flexible que la firma digital, y el Decreto 333, del 19 de febrero de 2014, que reglamenta las condiciones de constitución y funcionamiento de las entidades de certificación digital, modernizando su metodología de acreditación, sustituyendo este último al Decreto 1747 de 2000.

La Ley 527 establece que, en toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a la información suministrada en forma de un mensaje de datos, por el solo hecho de constar en ese formato o en razón de no haber sido presentada en su forma original. El valor probatorio de los mensajes de datos se determina de conformidad con las disposiciones conducentes del Código de Procedimiento Civil. Cabe señalar que Colombia ha suscrito la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (2005); sin embargo, todavía no ha sido ratificada.

En virtud del Decreto Ley 019, del 10 de enero de 2012, la función de autorización de las entidades de certificación ha sido sustituida por la función de acreditación a cargo del Organismo Nacional de Acreditación de Colombia, que sustituye a la Superintendencia de Industria y Comercio en esa labor. La acreditación de Entidades de Certificación es una función que ha sido también reglamentada por el Decreto 333 de 2014, y a la fecha de redacción del presente documento se encuentran pendientes por parte de ese Organismo la definición de los Criterios Específicos de Acreditación que regulen dicha materia. La vigilancia sobre la actividad de certificación digital se mantiene en la Superintendencia de Industria y Comercio.

En el ámbito administrativo, la Ley 962 de 2005, fechada el 8 de julio de 2005, por la cual se dictan disposiciones sobre la racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos, se establecen diversas medidas para facilitar las relaciones de los particulares con la Administración Pública. La Ley incorpora diversos principios rectores de la política de racionalización, estandarización y automatización de trámites para evitar exigencias injustificadas a los administrados, entre los que destaca el fortalecimiento tecnológico para articular la actuación de la Administración Pública y disminuir los

tiempos y costos de realización de los trámites por parte de los administrados. De igual forma, se incentiva el uso de medios tecnológicos integrados, para lo cual se faculta al Departamento Administrativo de la Función Pública, en coordinación con el Ministerio de Tecnología de la Información y las Comunicaciones, para orientar el apoyo técnico requerido por las entidades y organismos de la Administración Pública. La facturación electrónica es uno de los servicios que encuentran su fundamento en esa ley.

En materia de administración pública electrónica es destacable el desarrollo de la Ley 1437, del 18 de enero de 2011, Código de Procedimiento Administrativo y de lo contencioso administrativo que desarrolla en un capítulo independiente (III) lo relativo al procedimiento administrativo electrónico. En la precitada norma se destacan el procedimiento de notificación electrónica que prescinde totalmente de la presencialidad del interesado; la sede electrónica como mecanismo para agilizar el desarrollo de trámites y solicitud de servicios; el expediente electrónico y las sesiones virtuales. En lo relativo al expediente electrónico, esta disposición ya ha sido reglamentada por el Gobierno nacional a través del Decreto 2609, del 14 de diciembre de 2012.

Adicionalmente, la Ley 588, del 5 de julio de 2000, por medio de la cual se reglamenta el ejercicio de la actividad notarial, faculta a notarías y consulados, previa gestión ante la Superintendencia de Industria y Comercio, para actuar como entidades de certificación, de conformidad con la Ley 527 de 1999. En este sentido, se les permite transmitir en forma de mensajes de datos, por los medios electrónicos, ópticos y similares, copias, certificados y constancias de los documentos que tengan en sus archivos a otros notarios o cónsules. La Ley confiere a dichos documentos el carácter de auténticos.

Por su parte, el Decreto 624, del 30 de marzo de 1989, que expide el Estatuto Tributario, reglamenta la utilización de la factura electrónica y los documentos equivalentes a la factura de venta. En este sentido, el Decreto 1929, del 29 de mayo de 2007, por el cual se reglamenta el artículo 616-1 del Estatuto Tributario, define el concepto de factura electrónica y regula diversos aspectos vinculados con la expedición y la validez de las facturas de venta electrónicas, autorizando a las personas obligadas a facturar a utilizar medios electrónicos para su expedición.

En el ámbito de las operaciones aduanales, mediante Decreto 4149, del 10 de diciembre de 2004, se crea la "Ventanilla Única de Comercio Exterior (VUCE), ad-

ministrada por el Ministerio de Comercio, Industria y Turismo, y soportada en medios electrónicos por medio de los cuales las entidades administrativas relacionadas con las operaciones de comercio exterior comparten información, a efectos de tramitar autorizaciones y permisos relacionados con la importación y la exportación de bienes. La VUCE incorpora el uso de firmas digitales y de pagos electrónicos, basados en documentos XML, con los cuales se desmaterializan los documentos y trámites relacionados con las autorizaciones previas a las importaciones y exportaciones del país.

#### b) Protección al consumidor

En el ámbito de la Protección al Consumidor, la Constitución Política de Colombia consagra el derecho de los consumidores para que los bienes y servicios que les son suministrados en el mercado no atenten contra su salud y seguridad. De igual forma, se reconoce el derecho de los consumidores a recibir servicios públicos eficientes. Respecto de la protección del consumidor electrónico, un importante referente es la Ley 1480, del 12 de octubre de 2011, nuevo estatuto de protección al consumidor que desarrolla un capítulo completo en materia de comercio electrónico, regulando con especial suficiencia la relación entre empresarios y consumidores, destacando los deberes de información, lealtad y prudencia en el ofrecimiento de bienes a través de medios electrónicos. La autoridad de vigilancia es la Superintendencia de Industria y Comercio.

#### c) Protección de datos personales

Con relación a la protección de datos personales, se destacan dos leyes: la Ley Estatutaria en materia de protección de datos personales (Ley N° 1581), del 17 de octubre de 2012, y la Ley de Hábeas Data Financiera (Ley N° 1266), del 31 de diciembre de 2008. Estas normas regulan el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países. Tienen por objeto garantizar el derecho de todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos, así como los demás derechos, libertades y garantías constitucionales relacionados con la recolección, tratamiento y circulación de datos personales. Estas normas se aplican a todos los datos de información personal registrados en un banco de datos, sean estos administrados por entidades públicas o privadas, sin perjuicio de las normas especiales que los regulen. Se exceptúan de esta Ley las bases de datos que

produce el Servicio de Inteligencia del Estado para garantizar la seguridad nacional interna y externa de Colombia, así como aquellos datos mantenidos en un ámbito personal o doméstico y los que circulan internamente, es decir, que no se suministran a otras personas jurídicas o naturales.

Entre los principales derechos reconocidos por esta Ley se incluye el “derecho al olvido”, que se traduce como el derecho que tienen los titulares de aquellos datos cuyo contenido haga referencia al tiempo de mora, tipo de cobro, estado de la cartera, y en general aquellos datos referentes a una situación de incumplimiento de obligaciones, para que se retiren esos datos una vez que concluya el periodo de permanencia de cuatro años, contados a partir de la fecha en que sean pagadas las cuotas vencidas, o haya sido pagada la obligación vencida. Concluido este plazo, la información debe ser retirada de los bancos de datos por el operador, de forma que los usuarios no puedan acceder o consultar dicha información de las centrales de riesgo. La Ley contiene un Título especial que regula las peticiones de consultas y reclamos.

En virtud del Decreto 1377, del 27 de junio de 2013, se reglamenta parcialmente la Ley N° 1581 y se establecen diversos requerimientos relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, y el ejercicio de los derechos de los titulares de la información.

#### d) Propiedad Industrial e Intelectual

En materia de propiedad intelectual, destaca la normatividad supranacional de la Comunidad Andina, particularmente la Decisión 351 de 1991 o Régimen Común sobre Derecho de Autor y Derechos Conexos, que reconoce la protección a los autores y demás titulares de derechos sobre las obras del ingenio, incluidos los programas de ordenador en el campo literario, artístico o científico, cualquiera que sea el género o forma de expresión y sin importar el mérito literario o artístico ni su destino. Asimismo, protege a los intérpretes o ejecutantes, a los productores de fonogramas y a los organismos de radiodifusión, en sus derechos conexos a los del autor en los países miembros. A nivel interno, destaca la Ley 23, del 28 de enero de 1982, sobre derechos de autor y el Decreto 162, del 22 de enero de 1996, que reglamenta la Decisión Andina 351, así como la Ley 44, del 5 de febrero de 1993, en relación con las sociedades de gestión colectiva de derechos de autor o de derechos conexos.

Adicionalmente, Colombia ha suscrito:

- el Tratado de Beijing sobre Interpretaciones y Ejecuciones Audiovisuales (2012);
- los Tratados de la OMPI sobre Derecho de Autor (WCT) y sobre Interpretación o Ejecución y Fonogramas (WPPT);
- el Convenio de Berna para la Protección de las Obras Literarias y Artísticas;
- el Convenio de Ginebra para la protección de los productores de fonogramas contra la reproducción no autorizada de sus fonogramas;
- la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma);
- el Convenio de Bruselas sobre la distribución de señales portadoras de programas transmitidas por satélite, y
- el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), administrado por la OMC.

#### e) Nombres de dominio

En materia de nombres de dominio, mediante la Ley 1065 de 2006, el dominio .co de Colombia es administrado por la Universidad de los Andes por delegación de la IANA y se rige por el principio de “primero en llegar, primero en recibir” establecido en la Reglamentación para el funcionamiento de Nombres de Dominio .co. De igual forma, el Ministerio de Tecnologías de la Información y las Comunicaciones, con fundamento en la competencia asignada por la Ley 1065, del 29 de julio de 2006, adoptó la Política uniforme de solución de controversias establecida por la ICANN.

#### f) Delitos Informáticos y Seguridad de la Información

En el ámbito penal, la Ley 1273, del 5 de enero de 2009, por medio de la cual se modifica el Código Penal de Colombia, incluye dentro de los bienes jurídicos tutelados la información y los datos que se preservan integralmente en los sistemas que utilicen las tecnologías de la información y las comunicaciones.

La Ley adiciona el Título “De la protección de la información y de los datos” y tipifica diversos delitos como el acceso abusivo a un sistema informático, la obstaculización ilegítima del mismo o de una red de telecomunicación, la interceptación de datos informáticos, el daño informático, el uso de software malicioso, la violación de datos personales y la suplantación de sitios web para capturar datos personales, considerando esta conducta como un atentado contra la confidencialidad, la integridad y la disponibilidad

de los datos y los sistemas informáticos. Adicionalmente, sanciona el hurto por medios informáticos y la transferencia no consentida de activos realizada a través de estos medios.

#### g) Iniciativas de ley Ley y retos

En la actualidad se están revisando dos iniciativas reglamentarias que merecen especial mención. Por una parte, existe un proyecto de Decreto sobre factura electrónica para su masificación y obligatoriedad y, por otra, se ha creado una iniciativa reglamentaria en materia de documento electrónico transferible que tiene por objeto regular los títulos valores electrónicos.

Colombia ha implementado diversas políticas públicas para promover la conectividad de sus nacionales, sin embargo, enfrenta aún el reto de la falta de apropiación de la tecnología por parte de los empresarios en sus cadenas productivas. También es preciso trabajar en la armonización interna de la normatividad sobre los temas asociados a las TIC, pues existe una proliferación de disposiciones aplicables a las empresas que no se alcanzan a comprender y/o aplicar.

## COSTA RICA

En el marco de la normativa costarricense que regula el comercio electrónico se encuentra la Ley de Certificados, Firmas Digitales y Documentos Electrónicos (Ley N° 8454), fechada el 13 de octubre de 2005, el Código Civil (Ley N° 63), el Código de Comercio (Ley N° 3284), del 30 de abril de 1964, y la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor (Ley N° 7472), del 20 de diciembre de 1994, las cuales se revisan en los siguientes apartados junto con otros ordenamientos relevantes.

#### a) Transacciones electrónicas / Firmas electrónicas

En materia de transacciones electrónicas, el Código de Comercio (Ley N° 3284) que rige los actos de comercio y el Código Civil (Ley N° 63) que regula la formación de los contratos, entre presentes y entre ausentes, así como el momento y lugar en que se perfeccionan y las formalidades que deben revestir, se complementan con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos (Ley N° 8454), que reconoce el uso y la validez de los medios electrónicos para contratar.

La Ley N° 8454 incorpora algunos principios de la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas y establece el marco jurídico general para la utilización transparente, confiable y segura de los documentos electrónicos y la firma digital por parte de las entidades públicas y privadas, esto es: i) aplica a toda clase de transacciones y actos jurídicos, públicos o

privados, salvo disposición legal en contrario, o que la naturaleza o los requisitos particulares del acto o negocio concretos resulten incompatibles; ii) faculta expresamente al Estado y a todas las entidades públicas para utilizar los certificados, las firmas digitales y los documentos electrónicos, dentro de sus respectivos ámbitos de competencia; iii) reconoce la emisión de certificaciones, constancias y otros documentos; iv) la presentación, tramitación e inscripción de documentos en el Registro Nacional, y v) la gestión, conservación y utilización de protocolos notariales.

Por su parte, el Decreto Ejecutivo N° 33018-MICIT, del 20 de marzo de 2006, emite el Reglamento a la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, que define, entre otras cuestiones, las funciones y jerarquías que deben tener los distintos certificado es, partiendo del Certificador Raíz, así como las características y funciones de la Infraestructura de Llave Pública. De igual forma, establece los lineamientos técnicos que deben cumplir los certificados registrados en cuanto a su idoneidad técnica y administrativa.

En materia de contrataciones públicas, la Ley de Contratación Administrativa (Ley N° 7494), del 8 de junio de 1995, incorpora el uso de comunicaciones electrónicas en el procedimiento de contratación por parte de la Administración Pública, siempre que garantice la certeza de la recepción y el contenido de los mensajes. Asimismo, el Reglamento para la Utilización del Sistema de Compras Gubernamentales Compra RED, por Decreto Ejecutivo N° 32717, fechado el 24 de octubre de 2005, y el Reglamento para la Utilización del Sistema Electrónico de Compras Públicas Mercado en Línea “Mer-Link”, por Decreto Ejecutivo N° 36242-MP-PLAN, del 21 de octubre de 2010, dan a conocer en forma electrónica las solicitudes de bienes, obras y servicios; los registros electrónicos de proveedores y las etapas, decisiones y resultados de las compras del Estado, desde su inicio hasta su finiquito, permitiendo a los proveedores potenciales, a los ciudadanos y al propio Gobierno conocer en línea la información pertinente.

Por Decreto Ejecutivo N° 38830-H-MICITT, del 15 de enero de 2015, se crea el Sistema Integrado de Compras Públicas (SICOP) como la plataforma tecnológica de uso obligatorio para la Administración Central en los procedimientos de contratación administrativa. Compra RED y “Mer-Link” pueden ser utilizadas por las instituciones descentralizadas que voluntariamente las implementen.

En el ámbito de la Administración Pública, destaca la Directriz N° 067-MICITT-H-MEIC “Masificación de

la implementación y el uso de la firma digital en el Sector Público Costarricense”, fechada el 25 de abril del 2014, que ordena a las instituciones del sector público instrumentar medidas técnicas y financieras que permitan a los ciudadanos obtener información, realizar consultas, formular solicitudes, manifestar su consentimiento y compromiso, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos mediante el uso de medios electrónicos.

#### b) Protección al consumidor

En materia de protección al consumidor, la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor (Ley N° 7472) incorpora los principios básicos de las relaciones de consumo previstos en la Resolución 39/248 sobre las Directrices para la Protección al Consumidor, aprobada por la Asamblea General de las Naciones Unidas. La Ley N° 7472 regula, entre otras cuestiones, las obligaciones de los comerciantes frente a los consumidores en materia de información, publicidad u ofertas al público de bienes ofrecidos o servicios por prestar. Asimismo, establece las medidas de protección administrativa y judicial contra la publicidad engañosa, las prácticas y las cláusulas abusivas, los métodos comerciales desleales o que restrinjan la libre elección.

Con el Reglamento a la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor, emitido mediante Decreto Ejecutivo N° 37899-MEIC, fechado el 23 de septiembre de 2013, se amplió el concepto de “medio de difusión” con el fin de incluir al correo electrónico y otros medios de comunicación electrónica, informática y de telecomunicaciones para el envío de materiales publicitarios. De igual forma, se regula el derecho de retracto, que se puede ejercer a través del envío de correo electrónico dentro de los ocho días posteriores a la fecha del perfeccionamiento de la venta.

#### c) Protección de datos personales

Por lo que se refiere a la privacidad y protección de datos, Costa Rica ha adoptado la Declaración Universal de los Derechos Humanos y la Convención Interamericana de Derechos Humanos – Pacto de San José de Costa Rica, que reconocen como derecho fundamental el derecho a la intimidad y a la vida privada y que también se refleja en su Constitución.

En el ámbito de la legislación nacional, la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales (Ley N° 8968), fechada el 5 de septiembre de 2011, desarrolla el marco normativo que rige el tratamiento de los datos personales por parte

de los individuos, las instituciones públicas y privadas y que es conforme con las Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana emitidas por la Red Iberoamericana de Protección de Datos Personales. La Ley tutela el derecho a la autodeterminación informativa en relación con la vida o actividad privada de los interesados respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.

También establece que toda base de datos, pública o privada, administrada con fines de distribución, difusión o comercialización, debe inscribirse en el registro que al efecto habilite la Agencia de Protección de Datos de los Habitantes (Prodhab), y se le debe pagar un canon anual de regulación y administración de bases de datos de doscientos dólares (\$200), moneda de curso legal de los Estados Unidos de América. Asimismo, señala que en el caso de los contratos globales de bajo, medio y alto consumo de consultas a la base de datos registrada, o de las modalidades contractuales de servicio en línea por número de aplicaciones, el Reglamento determina el canon aplicable que no podrá ser superior al diez por ciento (10%) del precio contractual.

Por su parte, el Decreto Ejecutivo No. 37554-JP “Reglamento a la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales”, fechado el 5 de marzo de 2013, determina con mayor detalle: i) las medidas de seguridad que los responsables deben instrumentar para proteger los datos personales; ii) el proceso de inscripción de las bases de datos en la Prodhab; iii) el monto de los cánones atendiendo al nivel de consumo de consultas de la base de datos, y iv) los temas probatorios.

#### d) Propiedad Industrial e Intelectual

En el ámbito de la propiedad intelectual, destaca la Ley de Derechos de Autor y Derechos Conexos (Ley N° 6683), fechada el 14 de octubre de 1982, reformada por la Ley N° 8834, del 3 de mayo de 2010, que protege las obras artísticas y literarias, así como los programas de cómputo y las bases de datos, como compilaciones. Por su parte, el Decreto N° 36880-COMEX- JP, Reglamento sobre la limitación a la responsabilidad de los proveedores de servicios por infracciones a Derechos de Autor y Conexos, de acuerdo con el Artículo 15.11.27 del Tratado de Libre Comercio entre la República Dominicana, Centroamérica y Estados Unidos, fechado el 16 de junio de 2011, establece los casos en los que la responsabilidad de los Proveedores de Servicios de Almacenamiento Temporal o Caching, Alojamiento o Hosting, Conexión y Vinculación se limita respecto de

los materiales almacenados o transmitidos a través de sus sistemas o redes.

En cuanto a la propiedad industrial, cabe mencionar la Ley de Patentes de Invención, Dibujos y Modelos Industriales (Ley N° 6867), fechada el 25 de abril de 1983, modificada por última vez por la Ley N° 8632, de 25 de marzo de 2008, que no considera como invenciones susceptibles de patente a los métodos matemáticos ni a los programas de ordenador considerados de manera aislada, y la Ley de Información No Divulgada (Ley N° 7975), fechada el 4 de enero de 2000.

Con relación al ámbito internacional de los derechos de propiedad intelectual, es preciso señalar que Costa Rica ha ratificado

- los Tratados de la OMPI sobre Derecho de Autor (WCT) y sobre Interpretación o Ejecución y Fonogramas (WPPT);
- el Tratado de Beijing sobre Interpretaciones y Ejecuciones Audiovisuales (2012);
- el Protocolo al Convenio Centroamericano para la Protección de la Propiedad Industrial;
- el Tratado de Libre Comercio entre la República Dominicana, Centroamérica y Estados Unidos;
- el Arreglo de Lisboa relativo a la Protección de las Denominaciones de Origen y su Registro Internacional;
- el Convenio de París para la Protección de la Propiedad Industrial (1883);
- el Convenio de Berna para la Protección de las Obras Literarias y Artísticas;
- el Convenio de Ginebra para la protección de los productores de fonogramas contra la reproducción no autorizada de sus fonogramas;
- la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma), y
- el Convenio de Bruselas sobre la distribución de señales portadoras de programas transmitidas por satélite.

También ha suscrito el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), administrado por la Organización Mundial del Comercio (OMC).

#### e) Nombres de dominio

En materia de nombres de dominio, la Academia Nacional de las Ciencias, a través de su dependencia NIC-Internet Costa Rica (<http://nic.cr>), es la

entidad encargada de administrar y coordinar el funcionamiento del dominio de nivel superior .cr y en su Política de eliminación del dominio establece que ante un conflicto por un nombre de dominio registrado bajo el .cr, el NIC-Internet Costa Rica procederá a eliminar el nombre del dominio cuando así lo dicte la sentencia en firme de un tribunal nacional o extranjero. El procedimiento no aplica la Política uniforme de solución de controversias en materia de nombres de dominio de la ICANN.

#### f) Delitos Informáticos y Seguridad de la Información

En virtud de la Ley de Delitos Informáticos (Ley N° 9.048) y otras reformas al Código Penal, fechada el 6 de noviembre de 2012, se incluyeron diversos delitos informáticos que sancionan a: i) la persona que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, acceda, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes electrónicos, informáticos, magnéticos y telemáticos; ii) la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema, y iii) la persona que por cualquier medio acceda, borra, suprima, modifique o inutilice sin autorización los datos registrados en una computadora.

Por su parte, la Ley General de Aduanas (Ley N° 7557), fechada el 20 de octubre de 1995, tipifica diversos delitos informáticos cometidos en agravio de los sistemas utilizados por el Servicio Nacional de Aduanas.

#### g) Iniciativas de Ley y retos

Entre las iniciativas de Ley que merecen especial atención se encuentran las referentes a las leyes procesales en materia penal para facilitar la recolección y el tratamiento de pruebas en medios electrónicos. En el contexto internacional, la ratificación de la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales, así como del Convenio del Consejo de Europa sobre la Ciberdelincuencia, es una tarea que no se ha concretado.

## CUBA

El desarrollo del comercio electrónico en Cuba constituye una importante área de oportunidad para

potenciar los beneficios de las TIC en su economía, a través del despliegue de infraestructura tecnológica y de normativa que le dé sustento.

#### a) Transacciones electrónicas / Firmas electrónicas

A nivel de regulación, el tema del comercio electrónico y de las firmas electrónicas se ha desarrollado a través de la regulación administrativa emitida por diversas entidades del Poder Ejecutivo. Destacan los “Lineamientos para el desarrollo en Cuba del Comercio Electrónico”, fechados el 26 de diciembre de 2005, del Acuerdo del Consejo de Ministros, así como la Resolución 61/2002 del Banco Central de Cuba, fechada el 14 de noviembre de 2002, que establece las Normas para la ejecución de los cobros y pagos de las transacciones de comercio electrónico.

#### b) Protección al consumidor

En el ámbito de la protección al consumidor, Cuba no cuenta con una ley en la materia, aunque los temas conexos se atienden en el contexto del Sistema de Protección al Consumidor, vigente desde 2001, el cual rige a las entidades que realizan comercio minorista. Cabe señalar que en el Sistema no está expresamente comprendido el tema del comercio electrónico. Adicionalmente, el Código Penal (Ley N° 62), fechado el 29 de diciembre de 1987, sanciona algunas conductas que lesionan los intereses de los consumidores y que más adelante se describen.

#### c) Protección de datos personales

En el marco legal de Cuba no existe un reconocimiento expreso al derecho a la protección de datos personales, por consiguiente, se adolece de mecanismos o vías para su protección; solo a nivel de la regulación administrativa emitida por el Ministerio de la Informática y las Comunicaciones (MIC) se han incorporado algunas alternativas de tutela para los datos personales. Destaca la Resolución 57/1996 del MIC que crea el Registro Nacional de Información Electrónica para Redes de Datos, así como la Resolución 188/2001 del MIC, fechada el 15 de diciembre de 2001, que establece la Metodología para el Acceso de las Entidades Cubanas a Internet u otras Redes de Datos Externas.

#### d) Propiedad industrial e intelectual

En el ámbito de la propiedad intelectual destaca la Resolución Conjunta 1-99 del Ministerio de Cultura (MINCULT)-SIME para la Protección del Software por Derechos de Autor, fechada el 21 de junio de 1999, que establece el reglamento para la protección de programas de computación y bases de datos. La Resolución tiene el mérito de consagrar el principio de

protección acumulada de los derechos de autor y de propiedad industrial, en virtud del cual ambos sistemas se consideran independientes y compatibles.

En el contexto internacional es preciso señalar que Cuba ha suscrito:

- el Convenio de París para la Protección de la Propiedad Industrial;
- el Convenio de Berna para la Protección de las Obras Literarias y Artísticas, y
- el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio, de la OMC.

#### e) Nombres de dominio

En torno a la normativa de nombres de dominio, se destacan las siguientes resoluciones del Ministerio de Comercio: la Resolución 93/2003 - “Dominio.cu en servidores en Cuba”, fechada el 15 de octubre de 2003, que establece que los sitios web cubanos que utilizan el dominio “.cu” deben estar ubicados en servidores de Cuba, independientemente de estar también hospedados en servidores en el exterior del país. Asimismo, la Resolución 150/2008 - “Responsabilidad del CUBA-NIC y dominios genéricos” dispone que el Centro de Información de Red “CUBA-NIC” es el responsable de la correcta administración y gestión del dominio “.cu”, del funcionamiento de los servidores de nombre de dominios primarios y secundarios del Registro de Nombres de Dominios de segundo nivel bajo el “.cu” y del Registro de los Dominios de categorías genéricas bajo el dominio “.cu”.

Con la Resolución 72/2013 del Ministerio de la Informática y las Comunicaciones (MIC) se expide el Reglamento de Nombres de Dominio que establece las reglas para ordenar el sistema de asignación y registro de los nombres de dominios de las entidades. Faculta a la Agencia de Control y Supervisión del MIC para velar por que el sistema de nombres de dominio de Cuba constituya un servicio distribuido, jerárquico y escalable con control descentralizado. Asimismo, fija medidas en caso de incumplimientos al reglamento por los órganos y organismos, incluyendo la invalidación temporal o definitiva de las licencias de operación y/o la suspensión de los servicios.

#### f) Delitos Informáticos y Seguridad de la Información

El Código Penal, mediante la Ley N° 62, no hace referencia a los delitos informáticos, sin embargo, tipifica como delitos diversas conductas que atentan contra las normas de protección a los consumidores, entre otros: i) la venta al público de artículos incompletos en su composición o peso o deteriorados o en mal

estado de conservación; ii) el cobro de mercancías o servicios por encima del precio o tarifa aprobados por la autoridad u organismo competente, o del precio pactado por las partes; iii) la venta de productos industriales o agrícolas con indicación de calidad o designación de marca que no corresponda al producto, y iv) la utilización ilegal de una marca, modelo industrial o patente, en algún producto.

En cuanto a la seguridad de la información, la Resolución N° 127/2007 del MIC, fechada el 9 de julio de 2007, introduce al marco normativo el Reglamento de Seguridad para las Tecnologías de la Información. Por su parte, el Acuerdo N° 6058 del Comité Ejecutivo del Consejo de Ministros emitió los Lineamientos para el Perfeccionamiento de la Seguridad de las Tecnologías de la Información del 9 de julio de 2007.

#### g) Iniciativas de Ley y retos

Entre los proyectos normativos que se encuentran en proceso de revisión se tiene el proyecto de Decreto Ley "Normas Generales para la Práctica del Comercio Electrónico", el cual contiene, entre otras medidas, disposiciones para regular la transmisión y recepción de los mensajes de datos, los negocios jurídicos realizados a través de medios electrónicos, la protección de datos personales, así como las actividades, tanto de las autoridades de certificación y de registro como de las entidades certificadoras y los registros de certificación.

Adicionalmente, se encuentran en proceso de revisión tanto el proyecto de Ley sobre Infraestructura de Clave Pública como el Proyecto de reforma al Código Penal para incluir diversos delitos informáticos y el proyecto de reforma a la Ley de Derecho de Autor (Ley N° 14).

Entre los principales retos que enfrenta Cuba cabe mencionar la brecha digital y la falta de conectividad, aunado a la necesidad de aumentar las capacidades relacionadas con el conocimiento de las TIC en la población y en las instancias gubernamentales. Otro factor que ha inhibido el desarrollo de la conectividad en Cuba ha sido el embargo comercial impuesto al país desde hace 50 años por Estados Unidos de Norteamérica.

## ECUADOR

En materia de comercio electrónico, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (LCE) o Ley N° 2002-67, fechada el 17 de abril de 2002, es el principal instrumento normativo que regula los temas referentes a la contratación y firma

electrónica, así como los temas de protección al consumidor en línea.

#### a) Transacciones electrónicas / Firmas electrónicas

La LCE toma como referencia la Ley Modelo de la CNUDMI sobre Comercio Electrónico, así como la Directiva sobre comercio electrónico y la Directiva sobre firmas electrónicas del Consejo de Europa. La Ley confiere el mismo valor jurídico a los mensajes de datos respecto de los documentos escritos y a la firma electrónica respecto de la firma manuscrita. También regula los requisitos que debe cumplir la información consignada en un mensaje de datos para considerarse original.

La Ley autoriza la desmaterialización de documentos siempre que contengan una firma electrónica debidamente certificada. También señala los requisitos que deben cumplir la firma electrónica y los certificados de firma electrónica, así como las obligaciones y responsabilidades de las entidades de certificación de información acreditadas. La Ley acepta como medios de prueba los mensajes de datos, las firmas electrónicas, los documentos electrónicos y los certificados electrónicos nacionales o extranjeros, en las condiciones establecidas en la misma Ley. De igual forma, establece las sanciones administrativas y penales que corresponden en caso de incumplimiento.

Por su parte, el Reglamento a la LCE por Decreto N° 3496 -2002, fechado el 31 de diciembre de 2002, señala los requisitos que debe cumplir un mensaje de datos para considerarse accesible para su posterior consulta y le reconoce el mismo valor que a los documentos escritos. También indica los elementos y principios que deben regir la infraestructura de firma electrónica y la operación de las entidades de certificación de información, así como los servicios de sellado de tiempo.

El referido Reglamento establece el régimen para la acreditación, registro y regulación de entidades habilitadas para prestar servicios de certificación de información y servicios relacionados, así como de los terceros vinculados. De igual manera, identifica las normas y los procesos aplicables a la prestación de servicios de certificación de información, la emisión de certificados de firma electrónica, así como el registro de datos y el sellado de tiempo. De igual forma, regula con mayor detalle la operación de la infraestructura de clave pública y faculta a las entidades, instituciones del Estado y a las empresas públicas para adquirir certificados de firma electrónica de las Entidades de Certificación de Información y Servicios Relacionados Acreditadas, de derecho público o privado.

En el ámbito de las transacciones electrónicas gubernamentales, la Ley Orgánica del Sistema Nacional de Contratación Pública (LOSNCP), fechada el 4 de agosto de 2008, regula los procedimientos de contratación electrónica que aplica a los organismos gubernamentales, y sienta las bases legales para instrumentar el Sistema Nacional de Contratación Pública (SNPC) para las adquisiciones del Estado y la contratación de servicios. Determina también los requisitos que deben cumplir los proveedores del Estado para concursar en procedimientos de licitación electrónica, así como de subasta inversa electrónica.

En virtud del Decreto Ejecutivo 149 - Gobierno Electrónico y Simplificación de Trámites, del 20 de noviembre de 2013, se define “gobierno electrónico” como el uso de las tecnologías de la información y comunicación por parte de las entidades para transformar las relaciones con los ciudadanos, entre entidades de gobierno y empresas privadas, a fin de mejorar la calidad de los servicios gubernamentales a los ciudadanos, promover la interacción con las empresas privadas, fortalecer la participación ciudadana a través del acceso a la información y servicios gubernamentales eficientes y eficaces y coadyuvar con la transparencia, participación y colaboración ciudadana. Mediante el Decreto, se promueven los planes de simplificación de trámites en la Administración Pública Central e Institucional bajo los principios de simplicidad, economía, legalidad, celeridad, presunción de veracidad, responsabilidad de la información, privacidad de la información personal/confidencialidad, transparencia, privilegio de controles posteriores, informalismo y principio pro-administrado, gratuidad e interconexión.

La interoperabilidad gubernamental se ha implementado mediante tres ejes: i) la automatización de trámites y optimización de procesos; ii) el registro de datos públicos, y iii) los datos financieros. Para la gestión documental entre entidades del sector público y privado, la Secretaría Nacional de la Administración Pública ha implementado el sistema QUIPUX.

En el ámbito financiero, el Código Orgánico Monetario y Financiero, fechado el 12 de septiembre de 2014, regula la gestión de la moneda electrónica en el país y faculta al Banco Central del Ecuador para llevar a cabo su implementación, monitoreo y evaluación. La Resolución de la Junta de Política y Regulación Monetaria y Financiera No. 005-2014-M, del 6 de noviembre de 2014, en materia de dinero electrónico, establece las normas que rigen el funcionamiento de este medio de pago, reconocido por los agentes económicos y gestionado privativamente por el Banco Central, el cual es utilizado en dispositivos electrónicos, móviles, electro-

mecánicos, fijos, tarjetas inteligentes, computadoras y otros medios producto del avance tecnológico.

En el ámbito fiscal, tanto el Código Tributario del 14 de junio de 2005, modificado el 9 de marzo de 2009, como la LCE establecen la validez de las notificaciones electrónicas. Por su parte, la LCE define el concepto de factura electrónica. Los servicios fiscales se encuentran alineados al criterio de “Eliminación de papeles y automatización de procesos”; en tal virtud, las entidades como el Servicio Nacional de Aduana del Ecuador (SENAE) y el Servicio de Rentas Internas (SRI) son ejemplos representativos de este objetivo. El SENAE implementó el sistema informático aduanero “Ecuapass” y la Ventanilla Única Ecuatoriana (VUE), con los cuales se desarrollaron sistemas inteligentes de control de riesgos, siendo primordial la protección de la seguridad del declarante a través de certificados de firma electrónica. Por otro lado, el SRI viabiliza la presentación de declaraciones de impuestos vía Internet, los pagos en línea y la implementación de facturación electrónica.

#### b) Protección al consumidor

La Constitución de la República del Ecuador establece que las personas tienen derecho a disponer de bienes y servicios de óptima calidad y a elegirlos con libertad, así como a recibir información precisa y no engañosa sobre su contenido y características. Igualmente, regula los mecanismos de control de calidad y los procedimientos de defensa de los consumidores, así como las sanciones en caso de vulnerar los derechos de los consumidores.

Por su parte, la Ley Orgánica de Defensa del Consumidor (LODC) (Ley N° 2000-21), fechada el 10 de julio de 2000, consagra el derecho a la protección de la vida, la salud y la seguridad de los consumidores respecto del consumo de bienes y servicios, así como el derecho a la protección contra la publicidad engañosa o abusiva. De igual manera, reconoce el derecho de los consumidores a recibir información adecuada, veraz, clara, oportuna y completa sobre los bienes y servicios.

La LCE dispone que, previamente a que el consumidor o usuario exprese su consentimiento para aceptar registros electrónicos o mensajes de datos, debe ser informado clara, precisa y satisfactoriamente sobre los equipos y programas que requiere para acceder a dichos registros o mensajes. Adicionalmente, establece los requisitos que deben acreditarse en torno a la información que se debe proporcionar al consumidor sobre las operaciones de comercio electrónico, incluida la publicidad y las promociones. De igual forma, regula los mecanismos para que los consumi-

dores puedan ser excluidos de las listas, cadenas de mensajes o bases de datos para el envío de mensajes de datos con información de cualquier tipo.

### c) Protección de datos personales

En materia de privacidad y datos personales, la Constitución tutela el derecho de las personas para que en ningún caso se pueda exigir o utilizar, sin su autorización, la información personal que les concierna, incluyendo la referente a sus creencias religiosas, filiación o pensamiento político o sobre datos referentes a su salud y vida sexual, salvo por necesidades de atención médica. Asimismo, garantiza el derecho al honor y al buen nombre de las personas. Adicionalmente, establece el derecho de toda persona a conocer y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, sea en soporte material o electrónico.

De igual forma, reconoce el derecho de los titulares de la información a conocer sobre el uso, la finalidad, el origen y destino de la misma. Las personas responsables de los bancos o archivos de datos personales pueden difundir la información archivada si cuentan con la autorización de su titular o si lo prescribe alguna disposición legal.

La Constitución establece que la persona titular de los datos puede solicitar al responsable de su tratamiento el acceso sin costo al archivo correspondiente, así como la actualización de sus datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo debe ser autorizado por la persona titular, se exige la adopción de medidas de seguridad. Asimismo, reconoce el derecho a la inviolabilidad y al secreto de la correspondencia física y virtual.

A este respecto, la LCE establece que los mensajes de datos deben protegerse bajo los principios de confidencialidad y reserva, y determina que toda violación a estos principios, incluyendo la intrusión electrónica, la transferencia ilegal de mensajes de datos o la violación del secreto profesional será castigada. De igual forma, ordena que para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requiere del consentimiento expreso del titular de los datos, a menos que estos provengan de fuentes accesibles al público. El titular de los datos tiene el derecho a seleccionar la información que vaya a compartir con terceros.

Por su parte, la Ley Orgánica del Sistema Nacional de Contratación Pública, del 4 de agosto de 2008, establece que los datos que se suministren al portal ([www.compraspublicas.gov.ec](http://www.compraspublicas.gov.ec)) se consideran confidenciales y únicamente pueden ser utilizados para los fines para los cuales el proveedor los haya proporcionado.

La Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, del 31 de marzo de 2010, establece las obligaciones para las instituciones del sector público y privado que actualmente o en el futuro administren bases o registros de datos públicos, sobre las personas naturales o jurídicas, sus bienes o patrimonio y para las usuarias o usuarios de los registros públicos. Los datos personales deben conservarse confidenciales y su acceso queda sujeto a la autorización del titular de los datos. Tanto las dependencias como las personas del sector privado que custodien datos personales deben establecer medidas de seguridad para preservar la reserva de los datos personales. El acceso a la información patrimonial precisa que el solicitante justifique y motive su requerimiento, declare el uso que hará de la misma y consigne sus datos básicos de identidad.

La Ley Orgánica del Sistema Nacional de Registro de Datos Públicos, del 31 de marzo de 2010, establece las obligaciones para las instituciones del sector público y privado que actualmente o en el futuro administren bases o registros de datos públicos, sobre las personas naturales o jurídicas, sus bienes o patrimonio y para las usuarias o usuarios de los registros públicos. Los datos personales deben conservarse confidenciales y su acceso queda sujeto a la autorización del titular de los datos. Tanto las dependencias como las personas del sector privado que custodien datos personales deben establecer medidas de seguridad para preservar la reserva de los datos personales. El acceso a la información patrimonial precisa que el solicitante justifique y motive su requerimiento, declare el uso que hará de la misma y consigne sus datos básicos de identidad.

### d) Propiedad industrial e intelectual

En materia de propiedad intelectual, la Constitución del Ecuador consagra el derecho de las personas a desarrollar su capacidad creativa, al ejercicio digno y sostenido de las actividades culturales y artísticas, y a beneficiarse de la protección de los derechos morales y patrimoniales que les correspondan por las producciones científicas, literarias o artísticas de su autoría.

Cabe mencionar que, en el ámbito internacional, Ecuador ha suscrito:

- los Tratados de la OMPI sobre Derecho de Autor y sobre Interpretación o Ejecución y Fonogramas (WPPT);
- el Convenio de Berna para la Protección de Obras Literarias y Artísticas;
- la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma), y
- la Convención Universal sobre Derecho de Autor y el Régimen Común sobre Derecho de Autor y Derechos Conexos, regulado en la Decisión 351 de la Comisión del Acuerdo de Cartagena, vigente para todos los países de la Comunidad Andina.

Asimismo ha ratificado el ADPIC de la OMC

En el contexto de la legislación nacional destaca la Ley de la Propiedad Intelectual, fechada el 8 de mayo de 1998, que protege los derechos de autor y los derechos conexos así como la propiedad industrial. En el ámbito de los derechos de autor, es importante

destacar la protección que se confiere a los programas de ordenadores y a las bases de datos.

#### e) Nombres de dominio

En materia de nombres de dominio, el NIC.ec es la entidad a cargo de la administración del dominio .ec por delegación de la IANA. El NIC.ec ha adoptado dentro de sus políticas de resolución de controversias sobre nombres de dominio el procedimiento arbitral previsto en la Política uniforme de solución de controversias en materia de nombres de dominio de la ICANN.

#### f) Delitos Informáticos y Seguridad de la Información

Los delitos informáticos han sido incluidos en el Código Orgánico Integral Penal (COIP), fechado el 10 de febrero de 2014, que sanciona: i) la violación a la intimidad cometida por quien, sin la debida autorización, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona; ii) la apropiación fraudulenta por medios electrónicos; iii) la reprogramación o modificación de información de equipos terminales móviles; iv) el intercambio, comercialización o compra de información de equipos terminales móviles; v) la supresión, alteración o suposición de la identidad y estado civil; vi) la revelación ilegal de base de datos; vii) la interceptación ilegal de datos; viii) la transferencia electrónica de activo patrimonial; ix) el ataque a la integridad de sistemas informáticos; x) los delitos contra la información pública reservada legalmente, y xi) el acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

En el ámbito procesal, el COIP establece las normas para la interceptación de las comunicaciones o datos informáticos mediante el mandato judicial y define el término “contenido digital”.

En materia de seguridad de la información destaca la Resolución JB-2012-2148 de la Junta Bancaria, del 26 de abril de 2012, que obliga a las instituciones financieras a incorporar medidas de seguridad en los canales electrónicos, incluyendo aquellos que permiten prestar servicios de banca móvil, a fin de garantizar que las transacciones realizadas a través de estos canales cuenten con los controles, medidas y elementos de seguridad para evitar eventos fraudulentos y garantizar la seguridad y calidad de la información de los usuarios, así como los bienes de los clientes a cargo de las instituciones controladas.

Asimismo, destaca el Acuerdo Ministerial N° 166 - Esquema Gubernamental de Seguridad de la Información, del 20 de septiembre de 2013, que obliga a

todas las dependencias de la Administración Pública Central e Institucional a instrumentar un Esquema Gubernamental de Seguridad de la Información (EGSI), cuyo contenido debe incluir los elementos siguientes: i) Política de Seguridad de la Información; ii) Organización de la Seguridad de la Información; iii) Gestión de los Activos; iv) Seguridad de los Recursos Humanos; v) Seguridad Física y del Entorno; vi) Gestión de Comunicaciones y Operaciones; vii) Control de Acceso; viii) Adquisición, Desarrollo y Mantenimiento de Sistemas de Información; ix) Gestión de los Incidentes de la Seguridad de la Información; x) Gestión de la Continuidad del Negocio, y xi) Cumplimiento.

#### g) Iniciativas de Ley y retos

Diversas iniciativas de Ley en materia de protección de datos se han discutido en la Asamblea Nacional a efectos de proponer un sistema normativo acorde con las Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana emitidas por la Red Iberoamericana de Protección de Datos Personales, aunque no se han materializado. Asimismo, en el ámbito de la seguridad de la información, no se ha concretado el establecimiento CSITR nacional para la atención de ciberamenazas.

## EL SALVADOR

En El Salvador se utilizan diversas leyes para regir los diferentes temas del comercio electrónico. En el ámbito sustantivo se aplican disposiciones del Código Civil, fechado el 14 de abril de 1860, reformado en múltiples ocasiones, siendo la última el 11 de octubre de 1993; el Código de Comercio, fechado el 31 de julio de 1970, y modificado por última vez el 8 de mayo de 2014; la Ley de Protección al Consumidor, fechada el 16 de mayo de 2006 y reformada por última vez el 19 de febrero de 2013; el Código Tributario, fechado el 22 de diciembre de 2000 y modificado por última vez el 21 de diciembre de 2009, y la Ley de Simplificación Aduanera, fechada el 13 de enero de 1999, reformada por última vez el 4 de julio de 2012.

Por lo que se refiere al ámbito procesal, el Código Procesal Civil y Mercantil, fechado el 27 de noviembre de 2008 y reformado el 31 de mayo de 2010, reconoce los datos, los recursos de almacenamiento de datos o de información, incluyendo los soportes magnéticos e informáticos como medios de prueba, y les confiere valor probatorio en los procesos judiciales.

#### a) Transacciones electrónicas / Firmas electrónicas

En materia de transacciones electrónicas y de firma electrónica, ni el Código Civil ni el Código de Comercio regulan de manera expresa la contratación

electrónica, sin embargo, las reglas aplicables a la formación y al perfeccionamiento de los contratos, así como las reglas que determinan las formalidades que deben revestir los contratos, son aplicables a las transacciones electrónicas.

En el ámbito mercantil y financiero existen diversas disposiciones expresas que reconocen la equivalencia funcional entre los documentos impresos con firma autógrafa y los documentos digitales con firma digital. Tanto la Ley de Bancos, del 30 de septiembre de 1999, modificada por última vez el 20 de abril de 2012, como la Ley de Anotaciones Electrónicas de Valores en Cuenta, de fecha 22 de marzo de 2002, reformada por última ocasión el 20 de abril de 2012, reconocen la validez jurídica de las transacciones electrónicas y el uso de la firma electrónica.

Por su parte, la Ley de Bancos regula la función de intermediación financiera y otras operaciones realizadas por los bancos, bajo la supervisión del Banco Central de Reserva de El Salvador y la Superintendencia del Sistema Financiero. Establece que las operaciones activas y pasivas, que realicen los bancos entre sí, podrán realizarse mediante el intercambio electrónico de datos. También confiere validez probatoria a los registros o bitácoras contenidas en los sistemas informáticos, así como a las impresiones que reflejen las transacciones efectuadas por los mismos registros de firmas digitales o de números de identificación personal de los participantes autorizados en dichos sistemas. Asimismo, establece la obligación de los bancos de aceptar las instrucciones electrónicas para efectuar operaciones de débito o de crédito.

En materia bursátil, la Ley de Anotaciones Electrónicas de Valores en Cuenta también reconoce el uso de medios electrónicos para llevar a cabo transacciones electrónicas. Establece que las anotaciones electrónicas en cuenta representan valores negociables mobiliarios, incorporados a un registro electrónico y no a un documento. Asimismo, señala que los valores desmaterializados o anotados, al igual que los títulos valores, son una especie de valor y reconoce que la representación por medio de anotaciones electrónicas en cuenta es obligatoria para los valores negociables en bolsa. Faculta a los emisores de acciones representadas por medio de anotaciones en cuenta para llevar un Registro Electrónico de Accionistas en sustitución del Libro de Registro de Accionistas.

El Código Tributario autoriza las declaraciones fiscales a través de redes de comunicación electrónicas, como Internet. Asimismo, faculta a la Administración Tributaria para acceder por medios propios a los sistemas de facturación de las entidades financieras o

similares, así como de los administradores de tarjetas de crédito.

La Ley de Simplificación Aduanera representa un importante avance para las transacciones electrónicas, pues incorpora medidas conformes con el Reglamento del Código Aduanero Uniforme Centroamericano (RECAUCA) y el CAFTA-RD, y contiene algunas disposiciones alineadas con la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas. Autoriza la transmisión vía electrónica de las declaraciones de mercancías, los certificados o certificaciones de origen, los manifiestos de carga, los conocimientos de embarque y cualesquiera otros documentos requeridos para realizar operaciones de comercio exterior. También autoriza el pago de las obligaciones tributarias aduaneras mediante la transferencia electrónica de fondos de las cuentas bancarias de los declarantes, agentes de aduanas o de terceros, a la cuenta corriente de la Dirección General de Tesorería.

Por otra parte, señala que el uso de medios informáticos y de la vía electrónica para el intercambio de información gozará de plena validez para la formulación, transmisión, registro y archivo de la declaración de mercancías, de la información relacionada con la misma y de los documentos que a ésta deban adjuntarse, así como para certificar el pago del adeudo, y que su utilización producirá los mismos efectos jurídicos que generaría la entrega de esa misma información en soportes físicos.

Para garantizar la autenticidad, confidencialidad e integridad de la información intercambiada en los sistemas que interactúan con los sistemas aduanales, y a efectos de impedir su posterior repudiación, la Ley establece los sistemas de certificación de la información transmitida, que serán operados por entidades certificadoras. La Ley establece, para el intercambio de la información general, que cada usuario autorizado contará con una pareja de claves o llaves únicas y correspondientes entre sí, que constituyen la firma digital o electrónica, que representa el sustituto digital de la firma manuscrita

#### b) Protección al consumidor

Por lo que respecta a la protección al consumidor, la Constitución de El Salvador reconoce la defensa del interés de los consumidores como un derecho fundamental. Derivado de la Carta Magna, el Poder Legislativo emitió la Ley de Protección al Consumidor, la cual incorpora diversos preceptos de la Resolución 39/248 sobre las Directrices de las Naciones Unidas para la Protección al Consumidor, entre los cuales destaca el derecho de los consumidores a la infor-

mación, así como el derecho al acceso a productos seguros.

Entre los derechos que la Ley reconoce para los consumidores cabe mencionar los siguientes: i) recibir información completa, precisa, veraz, clara y oportuna sobre las características de los productos y servicios; ii) recibir información sobre los riesgos y/o efectos secundarios, así como sobre las condiciones de la contratación; iii) prohibir la publicidad engañosa o falsa; iv) recibir educación en materia de consumo; v) libertad de elección y trato igualitario; vi) protección contra los riesgos de recibir productos o servicios que pongan en peligro la vida, salud o integridad; vii) reclamar y recibir compensación por vicios ocultos; viii) prohibición de prácticas y cláusulas abusivas, y ix) derecho a la lectura completa y explicación de las obligaciones y condiciones estipuladas en contratos y anexos. En enero de 2013, la Ley fue reformada a efectos de incluir el derecho de retracto sin responsabilidad para el consumidor dentro de los ocho días siguientes a la contratación, para el caso de los contratos a distancia, incluyendo los celebrados a través de medios electrónicos.

### c) Protección de datos personales

En materia de protección de datos personales y del derecho a la vida privada, El Salvador ha suscrito la Convención Americana sobre Derechos Humanos y ha incorporado en su Constitución, como un derecho fundamental, el derecho a la vida privada en diversas disposiciones. Prohíbe la interferencia y la intervención de las telecomunicaciones, no obstante, autoriza de manera excepcional su intervención temporal mediante mandato judicial escrito y motivado.

Mediante la Ley del Nombre de la Persona Natural, del 4 de mayo de 1990, se establecen diversas medidas que protegen al titular de un nombre contra el uso indebido del mismo, sancionando la usurpación del nombre. Además, la Ley de Protección al Consumidor incluye medidas que protegen a los consumidores, al prohibir a los proveedores compartir información personal y crediticia del consumidor, ya sea entre proveedores o a través de entidades especializadas en la prestación de servicios de información, sin la debida autorización del consumidor. Establece obligaciones para las entidades especializadas en la prestación de servicios de información, las cuales están obligadas a permitir al consumidor el acceso a la información de sus datos, así como a solicitar la actualización, modificación y eliminación de los mismos, de forma gratuita. Asimismo, tendrán la obligación de corregir la información falsa, no actualizada o inexacta en un plazo

máximo de diez días contados a partir de la recepción de la solicitud del interesado.

En materia financiera, la Ley de Bancos establece que los depósitos y captaciones que reciben los bancos están sujetos a secreto y se podrá proporcionar informaciones sobre tales operaciones solo a su titular, a la persona que lo represente legalmente y a la Dirección General de Impuestos Internos cuando lo requiera en procesos de fiscalización. Dispone que el secreto bancario no será obstáculo para esclarecer delitos, para la fiscalización, determinación de impuestos o cobro de obligaciones tributarias, ni para impedir el embargo de bienes. La Ley de Bancos señala que la Superintendencia mantendrá un servicio de información de crédito sobre los usuarios de las instituciones integrantes del sistema financiero, con el objeto de facilitar a las mismas la evaluación de riesgos de sus operaciones.

Asimismo, la Ley de Regulación de los Servicios de Información sobre el Historial de Crédito de las personas, fechada el 27 de julio de 2011, reformada por última ocasión el 20 de abril de 2012, regula el tratamiento de los datos referentes al historial crediticio de los consumidores y clientes. La Ley tiene por objeto garantizar el derecho al honor, a la intimidad personal y familiar y a la propia imagen en el tema de la confiabilidad, la veracidad, la actualización y el buen manejo de los datos de consumidores o clientes, relativos a su historial de crédito, incorporados o susceptibles de ser incorporados a una agencia de información de datos administrada por una persona jurídica, debidamente autorizada conforme a la Ley. También regula la actividad de las personas jurídicas públicas o privadas, autorizadas para operar como agencias de información de datos y a los agentes económicos que mantengan o manejen datos sobre el historial de crédito de los consumidores o clientes.

Por su parte, la Ley de Anotaciones Electrónicas de Valores en Cuenta, ordena que los depósitos de valores que reciban las depositarias estarán sujetas a secreto y solo podrá proporcionarse información sobre esas operaciones a su titular o a la persona que lo represente legítimamente. Establece que el secreto bursátil no debe ser obstáculo para esclarecer delitos, ni para impedir embargos sobre bienes ni para la función de fiscalización de la Superintendencia.

En el ámbito aduanal, la Ley para la Simplificación Aduanera establece la obligación de mantener en secreto y reserva los datos personales o normativos de quienes firmen y sean certificados digitalmente. Asimismo, ordena que en ningún caso dichos datos personales podrán ser cruzados, perfilados o utiliza-

dos para otros fines que los regulados por dicha Ley, salvo que el titular de los datos consienta expresamente y por escrito en una finalidad distinta.

#### d) Propiedad industrial e intelectual

En materia de propiedad intelectual, la Constitución autoriza el otorgamiento de privilegios por tiempo limitado a los descubridores e inventores y a los perfeccionadores de los procesos productivos. En este sentido, la Ley de Propiedad Intelectual, fechada el 16 agosto de 1993, reformada por última ocasión el 20 de abril de 2012, protege bajo el régimen de los derechos de autor a las obras artísticas y literarias, entre ellas, los programas de ordenador y las compilaciones, dentro de las cuales se tienen en cuenta las bases de datos de ordenador. La Ley reconoce que cualquier almacenamiento permanente o temporal en forma electrónica de una obra se considera como una reproducción. En cuanto a los derechos conexos de artistas, intérpretes, ejecutantes y organismos de radiodifusión, define los conceptos de fonogramas y videogramas, y reconoce el derecho de comunicación pública por cualquier medio.

Por su parte, la Ley de Marcas y otros Signos Distintivos, del 8 de julio de 2002, modificada por última vez el 19 de abril de 2013, reconoce que los actos de competencia desleal, es decir, aquellos que se realizan en el ejercicio de una actividad mercantil o con motivo de ella, que sean contrarios a los usos y prácticas honestas en materia comercial, se pueden cometer a través de medios electrónicos de comunicación y de comercio. La Ley permite el uso de medios electrónicos para llevar a cabo el registro de signos distintivos. Tal disposición es conforme con la Ley de procedimientos uniformes para la presentación, trámite y registro o depósito de instrumentos en los Registros de la Propiedad Raíz e Hipotecas, Social de Inmuebles, de Comercio y de Propiedad Intelectual, que incorpora el uso del fax y de las direcciones electrónicas en las solicitudes de inscripción de instrumentos ante los registros para las notificaciones de los registradores a los solicitantes.

En el ámbito internacional, El Salvador ha ratificado

- los Tratados de la OMPI sobre Derecho de Autor (WCT) y sobre Interpretación o Ejecución y Fonogramas (WPPT);
- el Tratado de Beijing sobre Interpretaciones y Ejecuciones Audiovisuales (2012);
- la Convención Universal sobre Derecho de Autor;
- el Convenio de Bruselas sobre la distribución de señales portadoras de programas transmitidas por satélite;

- el Convenio Centroamericano para la Protección de la Propiedad Industrial;
- el Tratado de Libre Comercio entre la República Dominicana, Centroamérica y Estados Unidos, y
- el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), administrado por la Organización Mundial del Comercio (OMC).

#### e) Nombres de dominio

La Ley de Marcas y otros Signos Distintivos establece los requisitos y términos en que se protegen las marcas, los nombres comerciales, las denominaciones de origen y otros signos distintivos. La Ley es conforme con el CAFTA-RD y dispone que, tratándose de la piratería cibernética de marcas, la entidad nacional administradora del dominio de nivel superior de código del país (Asociación SVNet) debe contar con procedimientos para la resolución de controversias basados en los principios establecidos en la Política uniforme de solución de controversias en materia de nombres de dominio, y debe proporcionar acceso público en línea a una base de datos fiable y precisa con información de contacto para los registrantes de nombres de dominio, respetando las disposiciones legales relativas a la protección de la privacidad de los registrantes.

En este sentido, la Asociación SVNet (NIC-El Salvador), entidad encargada de emitir y actualizar las políticas para el funcionamiento del dominio de nivel superior .sv, ha incorporado su Política Uniforme para la Resolución de Controversias, así como su Reglamento, en virtud de los cuales establece las reglas que rigen los procedimientos arbitrales para la resolución de disputas en materia de nombres de dominio y reconoce al Centro de Mediación y Arbitraje de la Cámara de Comercio Americana (AMCHAM). Los instrumentos adoptados por la Asociación SVNet no hacen alusión a la Política uniforme de solución de controversias en materia de nombres de dominio de la ICANN.

#### f) Delitos Informáticos y Seguridad de la Información

En el ámbito penal, la Ley Especial contra Actos de Terrorismo, del 17 de octubre de 2006, reformada por última ocasión el 20 de noviembre de 2014, incluye algunos delitos informáticos. Así, se castiga al que para facilitar la comisión de cualquiera de los delitos previstos en la Ley en cuestión utilizare equipos, medios, programas, redes informáticas o cualquier otra aplicación informática para interceptar, interferir, desviar, alterar, dañar, inutilizar o destruir datos, información, documentos electrónicos, soportes informáticos,

programas o sistemas de información y de comunicaciones o telemáticos, de servicios públicos, sociales, administrativos, de emergencia o de seguridad nacional, de entidades nacionales, internacionales o de otro país. También castiga con la misma pena a la persona que creare, distribuyere, comerciare o tuviere en su poder programas capaces de producir los efectos previamente citados.

De igual forma, la Ley Especial para Sancionar Infracciones Aduaneras, fechada el 29 de octubre de 2001, reformada por última ocasión el 20 de abril de 2012, tipifica en su artículo 24 los siguientes delitos informáticos, que son sancionados con prisión de tres a cinco años, a quien: i) acceda sin la autorización correspondiente y, por cualquier medio, a los sistemas informáticos utilizados por la Dirección General de la Renta de Aduanas; ii) se apodere, copie, destruya, inutilice, altere, facilite, transfiera o tenga en su poder, sin autorización de la autoridad aduanera, cualquier programa de computación diseñado por o para tal autoridad o sus bases de datos, que de manera exclusiva y en el ejercicio de sus controles y servicios utilice la Dirección General; iii) dañe los componentes materiales o físicos de los aparatos, las máquinas o los accesorios que apoyen el funcionamiento de los sistemas informáticos o de comunicaciones, diseñados para las operaciones de la Dirección General, con la finalidad de entorpecerlas u obtener beneficio para sí o para otra persona; iv) facilite el uso del código y la clave de acceso, asignados para ingresar en los sistemas informáticos. La pena será de uno a tres años, si el empleo se facilita culposamente, y v) manipule el sistema informático o de comunicaciones a fin de imposibilitar cualquier control que, con base en dicho sistema, exista la posibilidad de realizar.

Además de los delitos informáticos previstos en la Ley Especial contra Actos de Terrorismo y la Ley Especial para Sancionar Infracciones Aduaneras, es preciso señalar que ni el Código Penal, del 10 de junio de 1997, modificada por última ocasión el 16 de octubre de 2014, ni el Código Procesal Penal, fechado el 30 de enero de 2009, modificado por última ocasión el 28 de enero de 2015, hacen referencia a los delitos informáticos ni a los mensajes de datos; sin embargo, las disposiciones de estos ordenamientos se aplicarían, dejando a la consideración de las autoridades ministeriales y judiciales la valoración de los elementos informáticos involucrados en los injustos penales.

#### g) Iniciativas de Ley y retos

El Salvador no cuenta con una estrategia nacional en materia de comercio electrónico, sin embargo, participa en el proyecto de la Autopista Mesoamericana

de la Información (AMI). Entre las principales iniciativas de Ley que se encuentran en proceso de revisión por parte de la Asamblea Legislativa, figura el anteproyecto de Ley para la Regulación del Comercio Electrónico, Documentos y Firma Digital. Actualmente, la Asamblea Legislativa está evaluando la propuesta de una nueva legislación con el nombre de Ley Especial contra el Delito Cibernético.

Entre los principales retos se encuentra el contar con una Ley general sobre Protección de Datos, que sea acorde con las Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana emitidas por la Red Iberoamericana de Protección de Datos Personales, así como la consolidación de un CERT nacional para la atención de incidentes de ciberseguridad.

## GUATEMALA

La Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, fechada el 23 de septiembre de 2008, constituye el principal ordenamiento que rige al comercio electrónico, no obstante lo anterior, en los ámbitos civil, mercantil, financie o administrativo y penal también resulta aplicable a determinados aspectos sobre el comercio electrónico que a continuación se desarrollan.

Asimismo, se encuentra en proceso de discusión una Agenda Digital que incluya estrategias para promover el comercio electrónico.

#### a) Transacciones electrónicas / Firmas electrónicas

En materia de transacciones electrónicas, destacan en el ámbito internacional el CAFTA-RD y el RECAUCA y, en el ámbito nacional, la Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas, la cual se aplica a todo tipo de comunicación electrónica, transacción o acto jurídico, sea público o privado, nacional o internacional, con las salvedades previstas en dicha ley.

La Ley para el Reconocimiento de las Comunicaciones y Firmas Electrónicas establece que el comercio electrónico abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de comunicaciones electrónicas o medios similares. La Ley incorpora diversos preceptos de Leyes Modelo de la CNUDMI sobre Comercio Electrónico y las Firmas Electrónicas. Asimismo, establece los requisitos jurídicos que deben cumplir las comunicaciones electrónicas, así como los elementos que deben concurrir para la formación y el perfeccionamiento de los contratos a través de medios electrónicos.

La Ley define también las características que deben cumplir las firmas electrónicas y los certificados digitales, así como las funciones de los prestadores de servicios de certificación que supervisa el Ministerio de Economía. Reconoce la equivalencia funcional de los documentos impresos con firma autógrafa respecto de los documentos en forma electrónica suscritos con firma electrónica avanzada y amparados por un certificado digital. Asimismo, establece disposiciones que regulan materias específicas, como el transporte de mercancías, e incorpora medidas en materia de protección al consumidor en línea.

En el Código Civil, fechado el 14 de septiembre de 1963, se establecen los principios que deben regir los contratos de adhesión y se reconoce la equivalencia funcional de la firma autógrafa y de la firma electrónica, digitalizada o impresa por cualquier medio electrónico, del registrador del Registro General de la Propiedad respecto de los asientos inscritos en los libros electrónicos.

El Código de Comercio, del 28 de enero de 1970, establece la obligación de conservar por cinco años la documentación e información relacionada con dichas actividades y de inscribir en el Registro Mercantil diversos actos en los libros o sistemas conducentes. En el ámbito financiero, la Ley Orgánica del Banco de Guatemala, fechada el 13 de mayo de 2002, faculta a ese instituto para procurar el buen funcionamiento del sistema de pagos de acuerdo con los lineamientos emanados de la Junta Monetaria. La Junta Monetaria emitió el Reglamento del Sistema de Liquidación Bruta en Tiempo Real (LBTR), fechado el 30 de noviembre de 2005, que regula, entre otras cuestiones, el uso de la firma digital. La Ley del Mercado de Valores y Mercancías, del 24 de junio de 1996, autoriza el control y manejo contable de las operaciones relacionadas con los valores representados por medio de anotaciones en cuenta mediante procedimientos contables, documentales o electrónicos.

En el ámbito de las transacciones electrónicas con el gobierno, la Ley de Contrataciones del Estado, del 31 de enero de 2009, establece las bases de operación del sistema de compras gubernamentales en línea denominado "Guatecompras". La Ley establece que, en los procesos de cotización y licitación, las entidades deben publicar en el sistema Guatecompras las bases de cotización o licitación, las especificaciones técnicas, los criterios de evaluación, las preguntas y respuestas, el listado de oferentes, las actas de adjudicación y los contratos de las contrataciones y adquisiciones. Asimismo, autoriza las notificaciones electrónicas por vía del sistema Guatecompras y

acepta que las modificaciones de las bases de cotización se publiquen en este sistema.

Además del Reglamento de la Ley de Contrataciones del Estado (que desarrolla las facultades de la Dirección Normativa de Contrataciones y Adquisiciones del Estado) así como el Acuerdo Ministerial 1-2006 Vinculación del Sistema de Gestión (SIGES), el Sistema de Contabilidad Integrada (SICOIN) y el sistema Guatecompras, destaca la Resolución N° 30-2009 de la Dirección Normativa de Contrataciones y Adquisiciones del Estado, la cual reconoce legalmente la dirección de Internet del Sistema de Información de Contrataciones y Adquisiciones del Estado ([www.guatecompras.gt](http://www.guatecompras.gt)) y determina, entre otras cuestiones, el tipo de usuarios del sistema y la gestión de las cuentas de acceso al mismo por parte de la Dirección Normativa antes mencionada.

En el ámbito fiscal, el Código Tributario, del 3 de abril de 1991, faculta a la Administración Tributaria para: i) establecer procedimientos para la elaboración, transmisión y conservación de facturas, libros, registros y documentos por medios electrónicos, y ii) requerir a los contribuyentes que presenten el pago de los tributos por medios electrónicos. También faculta a los contribuyentes para dar cumplimiento a sus obligaciones fiscales mediante uso de formularios electrónicos y les permite presentar declaraciones (entre ellas, las declaraciones juradas), estados financieros, sus anexos o cualquier información que estén obligados a proporcionar conforme a la ley, por vía electrónica, siempre que se identifiquen a través de una clave electrónica confidencial, que equivale a su firma autógrafa; que aseguren la integridad de la información presentada, o que la Administración Tributaria le entregue una constancia de recepción en forma física o electrónica.

Cabe mencionar que, de conformidad con el Código Tributario, tanto la Ley del Impuesto al Valor Agregado como la Ley del Impuesto sobre la Renta y sus respectivos Reglamentos Concordados admiten también el uso de medios electrónicos para la interacción de los contribuyentes con las autoridades fiscales y el cumplimiento de diversas obligaciones tributarias.

Finalmente, en el ámbito aduanero, Guatemala aplica a sus operaciones de comercio exterior el CAUCA y su Reglamento, así como el CAFTA-RD.

#### b) Protección al consumidor

Por lo que respecta a la protección al consumidor, la Constitución Política de la República de Guatemala establece la prohibición de prácticas excesivas que conduzcan a la concentración de bienes y medios de producción en detrimento de la colectividad, así como la defensa de los consumidores y usuarios en

cuanto a la preservación de la calidad de los productos de consumo interno y de exportación. Derivado del mandato constitucional de proteger el interés de los consumidores, se emitió el Decreto N° 6-2003 del Congreso de la República, que aprobó la Ley de Protección al Consumidor y Usuario, del 10 de marzo de 2003.

Por su parte, la Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor incorpora los principios básicos de las relaciones de consumo previstos en la Resolución 39/248 sobre las Directrices para la Protección al Consumidor, aprobada por la Asamblea General de las Naciones Unidas. La Ley establece que los derechos y garantías previstos en ella son de carácter irrenunciable y de orden público.

También reconoce entre otros derechos: i) el derecho a la seguridad de los consumidores; ii) el derecho a la información; iii) la libertad de contratación; iv) el derecho a la reparación, indemnización, devolución de dinero o cambio del bien por incumplimiento; v) el derecho a la educación sobre el consumo, y vi) el derecho de retracto sin responsabilidad, el cual puede ser ejercido dentro de los cinco días hábiles contados a partir de la fecha de la firma del contrato o desde la fecha en que este se hubiere celebrado fuera del establecimiento comercial, especialmente por teléfono o en el domicilio del consumidor o usuario. Cabe señalar que ninguna de estas leyes da un tratamiento especial para las operaciones en línea respecto de las operaciones tradicionales.

#### c) Protección de datos personales

En materia de protección de datos personales, la Constitución de Guatemala protege la vida privada al consagrar como derecho fundamental la inviolabilidad del secreto de la correspondencia y de las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna. También determina que toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad de tal información, así como a su corrección, rectificación y actualización. En igual sentido, el Código Tributario protege el secreto fiscal.

En el ámbito financiero, el Decreto N° 19-2002, Ley de Bancos y Grupos Financieros, fechado el 15 de mayo de 2002, regula el secreto bancario y dispone que, salvo las obligaciones y deberes establecidos por la normativa sobre lavado de dinero u otros activos, los directores, gerentes, representantes legales, funcionarios y empleados de los bancos no podrán revelar ninguna información.

El Decreto N° 57-2008, Ley de Acceso a la Información Pública, del 23 de octubre de 2008, tutela el derecho de toda persona individual a conocer y proteger los datos personales que sobre ella consten en archivos estatales, así como a su actualización. Establece el derecho del Hábeas Data como la garantía que tiene toda persona de ejercer el derecho para conocer lo que de ella conste en archivos, fichas, registros o cualquier otra forma de registros públicos, y la finalidad a que se dedica esta información, así como a su protección, corrección, rectificación o actualización. Los sujetos obligados no pueden difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información desarrollados en el ejercicio de sus funciones, salvo que hubiere mediado el consentimiento expreso por escrito de los individuos a que hiciera referencia la información. Asimismo, se prohíbe la comercialización por cualquier medio de datos sensibles o datos personales sensibles.

#### d) Propiedad industrial e intelectual

Los derechos de autor y el derecho de inventor se consagran constitucionalmente. La Ley de Derecho de Autor y Derechos Conexos, fechada el 19 de mayo de 1998, reformada por última ocasión el 27 de septiembre de 2000, tutela los derechos de los autores de obras artísticas, científicas y literarias. Considera dentro de las obras protegibles tanto a los programas de ordenador como a las bases de datos. De igual forma, reconoce que cualquier almacenamiento permanente o temporal en cualquier tipo de soporte material, formato o medio, una obra se considera como una reproducción. En cuanto a los derechos conexos de artistas, intérpretes, ejecutantes y organismos de radiodifusión, define los conceptos de fonogramas y videogramas, y reconoce el derecho de comunicación al público por cualquier medio o procedimiento, análogo o digital.

La Ley de Propiedad Industrial, del 18 de septiembre de 2000, no considera como invenciones susceptibles de patente a los métodos económicos, de publicidad o de negocios ni a los programas de ordenador considerados aisladamente.

El Código Penal, fechado el 27 de julio de 1973, castiga los siguientes delitos relacionados con la propiedad industrial y la propiedad intelectual: i) la atribución falsa de la calidad de titular de un derecho de autor, de artista, de intérprete, de productor de fonograma o de un organismo de radiodifusión; ii) la presentación, ejecución o audición pública o transmisión, comunicación, radiodifusión y/o distribución de una obra literaria o artística protegida, sin la autorización del titular; iii) la transmisión o la ejecución pública

de un fonograma protegido, sin la autorización de un productor; iv) la reproducción o arrendamiento de ejemplares de obras literarias, artísticas o científicas protegidas, sin la autorización del titular; v) la revelación de secretos industriales, y vi) el uso de marcas registradas o imitaciones de estas, entre otras.

En el ámbito internacional de los derechos de propiedad intelectual e industrial, Guatemala ha ratificado

- los Tratados de la OMPI sobre Derecho de Autor (WCT) y sobre Interpretación o Ejecución y Fonogramas (WPPT);
- el Tratado de Beijing sobre Interpretaciones y Ejecuciones Audiovisuales (2012);
- el Tratado de Libre Comercio entre la República Dominicana, Centroamérica y Estados Unidos;
- el Arreglo de Lisboa relativo a la Protección de las Denominaciones de Origen y su Registro Internacional;
- el Convenio de París para la Protección de la Propiedad Industrial (1883);
- el Convenio de Berna para la Protección de las Obras Literarias y Artísticas;
- el Convenio de Ginebra para la protección de los productores de fonogramas contra la reproducción no autorizada de sus fonogramas;
- la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma);
- el Tratado de la OMPI sobre Cooperación en Materia de Patentes –PCT, y
- el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), administrado por la Organización Mundial del Comercio (OMC).

#### e) Nombres de dominio

En materia de nombres de dominio, el Centro de Resolución de Nombres de Dominio para el Dominio de Nivel Superior .GT- Guatemala, perteneciente a la Universidad del Valle de Guatemala, es la entidad encargada de emitir y actualizar las políticas para el funcionamiento del dominio de nivel superior .gt, y ha adoptado los principios de la Política uniforme de solución de controversias en materia de nombres de dominio de la ICANN.

#### f) Delitos Informáticos y Seguridad de la Información

En el ámbito de los delitos informáticos, el Código Penal de Guatemala sanciona los siguientes: i) des-

trucción de registros informáticos; ii) alteración de programas; iii) reproducción ilícita de programas de computación; iv) creación de un banco de datos o un registro informático con datos que puedan afectar a la intimidad de las personas; v) utilización de registros informáticos o programas de computación para ocultar, alterar o distorsionar la información requerida para una actividad comercial, para el cumplimiento de una obligación respecto al Estado o para ocultar, falsear o alterar los estados contables o la situación patrimonial de una persona física o jurídica, y vi) la distribución de programas destructivos.

En materia de seguridad de la información, se cuenta con un CSIRT nacional que se ha creado sin las formalidades de Ley; sin embargo, se estima conveniente dotarle de facultades y recursos a través de instrumentos legales y/o reglamentarios.

#### g) Iniciativas de Ley y retos

Entre los principales retos que enfrenta Guatemala se encuentra la actualización del marco legislativo, en materia penal, tanto en el ámbito sustantivo como procesal, para robustecer las capacidades del Estado a los fines de combatir los delitos informáticos. Además, se están preparando modificaciones reglamentarias y jurídicas para posibilitar la creación y operación del CSIRT nacional dependiente del Ministerio del Interior. De igual forma, el marco normativo en materia de protección de datos requiere actualizarse para dar cumplimiento a los compromisos asumidos por Guatemala en la Red Iberoamericana de Protección de Datos.

## HAITÍ

En Haití no se cuenta con una ley que regule el comercio electrónico, sin embargo, está en proceso de debate parlamentario una iniciativa de Ley y en proceso de discusión una Agenda Digital, que incluye estrategias para promover el comercio electrónico.

#### a) Transacciones electrónicas / Firmas electrónicas

En la actualidad, Haití no cuenta con una ley sobre transacciones electrónicas ni sobre firmas electrónicas, siendo esta situación una importante área de oportunidad que debería tenerse en cuenta en el marco del proyecto HIPCAR.

#### b) Protección al consumidor

Haití no cuenta con una ley sobre protección al consumidor, sin embargo, está pendiente de revisión parlamentaria un proyecto de Ley en esta materia, fechado en 2010.

### c) Protección de datos personales

La Constitución de la República de Haití, del 10 de marzo de 1987, consagra como derechos fundamentales el derecho a la intimidad y a la vida privada. Sin embargo, no existe todavía una ley específica en materia de protección de datos. La incorporación de Haití a la Red Iberoamericana de Protección de Datos puede aportar mucho al proceso legislativo, con miras a emitir una Ley especial en la materia.

### d) Propiedad Industrial e Intelectual

La Constitución de Haití garantiza la protección de los derechos de propiedad intelectual. Sin embargo, el principal instrumento jurídico sobre la materia es el Decreto del 9 de enero de 1968 sobre los Derechos de Autor de obras Literarias, Científicas y Artísticas, que tutela la protección de los derechos morales y materiales de los autores respecto de las obras literarias, musicales y artísticas, y las obras cinematográficas y fotográficas. El Decreto no abarca expresamente todos los derechos conexos (derechos de productores de fonogramas o de organismos de radiodifusión, por ejemplo); tampoco abarca los programas de ordenador ni las bases de datos que, en virtud del Acuerdo sobre los ADPIC, están protegidos en tanto que obras literarias.

El Decreto reconoce a los titulares de los derechos de autor principalmente los derechos exclusivos de publicación, reproducción, representación, ejecución, adaptación, difusión, traducción, distribución y arreglo. También reconoce los derechos morales intangibles, inalienables e inembargables. La protección de los derechos de autor se extiende durante la vida del titular más 25 años después de su fallecimiento. La infracción de los derechos de autor puede entrañar, además de la confiscación de las copias falsificadas, la condena del autor de la falsificación a pagar indemnización por daños y perjuicios al titular de los derechos.

En el contexto internacional, Haití ha suscrito:

- el Convenio de París para la Protección de la Propiedad Industrial;
- el Convenio de Berna para la Protección de las Obras Literarias y Artísticas;
- la Convención Interamericana de Washington sobre el Derecho de Autor en Obras Literarias, Científicas y Artísticas,
- el Tratado sobre el Derecho de Patentes y el Tratado de Beijing sobre Interpretaciones y Ejecuciones Audiovisuales.

Adicionalmente, ha adoptado el Acuerdo sobre los ADPIC de la OMC.

### e) Nombres de dominio

La administración del dominio de nivel superior de código de país “.ht” está a cargo de la Red de Desarrollo Sostenible de Haití. En cuanto a políticas de resolución de controversias sobre nombres de dominio “.ht”, la Red no ha publicado una política alineada a la Política uniforme de solución de controversias de la ICANN.

### f) Delitos Informáticos y Seguridad de la Información

Haití no ha incluido delitos informáticos en su Código Penal de 1985, y el Código Procesal Penal tampoco incluye medidas para el manejo de evidencias digitales relacionadas con los delitos ni para su investigación.

### g) Iniciativas de Ley y retos

El estado de la ciberlegislación de Haití puede desarrollarse de manera notable con la participación del país en el proyecto HIPCAR, en los temas de comercio electrónico (transacciones), comercio electrónico (pruebas), privacidad y protección de datos, interceptación de comunicaciones, ciberdelincuencia y acceso a la información pública (libertad de información).

Entre los retos principales que enfrenta Haití se encuentra la falta de conectividad y de capacidades para el uso de las TIC.

## HONDURAS

En el marco de la Agenda Digital de Honduras 2014-2018, se plantea el fortalecimiento del marco legal en materia de comercio electrónico a efectos de impulsar su desarrollo, y se propone la creación de, entre otras leyes, una Ley sobre Comercio Electrónico que permita fortalecer el marco legal existente. Entre los principales ordenamientos en la materia se tiene la Ley sobre Firmas Electrónicas, mediante Decreto N° 149-2013, del 11 de diciembre de 2013, y la Ley de Compras Eficientes y Transparentes a través de Medios Electrónicos, mediante Decreto N° 36-2013, del 5 de agosto de 2014, que rige al sector público. El Código Civil, del 8 de febrero de 1906, reformado en 2009, también se aplica a la celebración, formalización, validez y eficacia de los contratos.

### a) Transacciones electrónicas / Firmas electrónicas

El Gobierno de Honduras ha suscrito la Convención de Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales y la ha incorporado en su derecho interno mediante Decreto N° 13-2009. Asimismo, ha

incorporado en la Ley sobre Firmas Electrónicas las disposiciones de la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas, reconociendo y regulando el uso de tales firmas a la información en forma de mensaje de datos, y otorgándoles la misma validez y eficacia jurídica que el uso de la firma manuscrita que conlleve manifestación de voluntad de los firmantes.

La Ley distingue la firma electrónica de la firma electrónica avanzada, confiriéndoles diferentes efectos jurídicos, y reconoce la equivalencia funcional de los documentos impresos respecto de los documentos consignados en mensajes de datos, así como de la firma manuscrita respecto de la firma digital, que ha sido certificada por un prestador de servicios acreditado. También faculta a las autoridades del Estado de los distintos poderes para llevar a cabo trámites administrativos a través de medios electrónicos y a utilizar expedientes electrónicos y firmas digitales en sus actuaciones, sea entre sí o con los particulares.

Por su parte, el Código de Comercio de mayo de 1950 faculta a los comerciantes para llevar su contabilidad en sistemas electrónicos, entre ellos, los libros de contabilidad y los libros y registros especiales, documentos, facturas, correspondencia enviada y recibida, así como los antecedentes de los hechos generadores de la obligación tributaria o, en su caso, los programas, subprogramas y demás registros procesados mediante sistemas electrónicos o de computación.

Asimismo, la Ley del Sistema Financiero, fechada el 22 de septiembre de 2004, permite a las instituciones del sistema ofrecer y prestar productos y servicios financieros por medios electrónicos, y reconoce los efectos jurídicos de la firma electrónica, la cual tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel, siempre que se base en un certificado reconocido y un código secreto que haya sido producido por un dispositivo seguro de creación de firma. Dicha firma será admisible como prueba en juicio y se valorará como instrumento público.

En materia administrativa, la Ley de Contratación del Estado, del 29 de junio de 2001, incorpora el uso de las tecnologías de la información en la gestión de los sistemas de contratación. Sin embargo, mediante la Ley de Compras Eficientes y Transparentes a través de Medios Electrónicos, por Decreto N° 36-2013, del 5 de agosto de 2014 (Ley de Compras), se amplían los supuestos de las compras de bienes o servicios de la Administración Pública para incluir las realiza-

das por Catálogo Electrónico, que comprende las modalidades de Convenio Marco, Compra Conjunta y Subasta Inversa que celebren los órganos de la Administración Pública Centralizada y Descentralizada.

De igual forma, la Ley de Propiedad, del 15 de junio de 2004, que rige los actos relacionados con la propiedad mueble, inmueble, mercantil e intelectual, así como los derechos reales y otros derechos, establece medidas para agilizar la gestión de los trámites relacionados y faculta al Registro Unificado de la Propiedad para aplicar instrumentos jurídicos, administrativos y tecnológicos avanzados que garanticen la seguridad, transparencia y reducción de los costos y tiempos para las transacciones registrables y de los procedimientos administrativos, entre otros, el uso de mecanismos destinados a la emisión de certificaciones electrónicas sobre actos, contratos o derechos que consten en expedientes públicos, teniendo los mismos, fuerza y valor probatorio de documentos públicos.

En materia fiscal, el Código Tributario, fechado el 30 de mayo de 1997, contiene diversas medidas que facilitan las transacciones en línea, como la emisión de comprobantes de actividades de los contribuyentes. Mediante el Reglamento del Régimen de Emisión y Generación de Documentos Fiscales Electrónicos, del 23 de octubre de 2014, se regulan los procedimientos, requisitos, condiciones y obligaciones de los contribuyentes Emisores o Generadores de Documentos Fiscales Electrónicos, a los cuales deben sujetarse los Emisores de Documentos Fiscales Electrónicos y los Generadores de Documentos Fiscales Electrónicos, debidamente autorizados por la Dirección Ejecutiva de Ingresos, para diversas modalidades de emisión y/o generación de documentos fiscales.

En materia aduanal, la Ley General de Aduanas, del 14 de diciembre de 1987, no contempla el uso de medios electrónicos para el despacho aduanal y sus trámites relacionados, sin embargo, reconoce la aplicación de los tratados internacionales, por lo que resultan aplicables el CAUCA y el RECAUCA que sí los consideran. De igual manera, es importante mencionar a la Ley de Implementación del Tratado de Libre Comercio entre la República Dominicana, Centroamérica y Estados Unidos, en virtud de la cual Honduras incorporó a su régimen interno las disposiciones del CAFTA-RD.

#### b) Protección al consumidor

En relación con la protección al consumidor, la Constitución de la República de Honduras, del 11 de enero de 1982, reformada por última ocasión el 4 de mayo

de 2005, obliga al Estado a reconocer, garantizar y fomentar la libertad de consumo. De conformidad con el mandato constitucional y con la Resolución 39/248 sobre las Directrices de las Naciones Unidas para la Protección al Consumidor, la Ley de Protección al Consumidor, fechada el 1 de abril de 2008, incorpora en la normativa de Honduras los derechos fundamentales de los consumidores a la información y al acceso a productos seguros (<http://www.lexadin.nl/wlg/legis/nofr/oeur/lxwehnd.htm>).

La Ley regula las “ventas por correspondencia y otras similares” incluyendo en las últimas a aquellas propuestas de venta, bienes o servicios efectuadas vía telecomunicaciones, o medios electrónicos cuya aceptación se realiza por iguales medios. Resultan aplicables a las transacciones en línea las medidas vinculadas con el derecho a la información clara –en español y con caracteres legibles–, veraz, completa y oportuna (entre otras, las relacionadas con el precio, la calidad y las garantías de los bienes y servicios), así como la prohibición de la publicidad engañosa y las cláusulas abusivas en los contratos de adhesión.

En virtud del Acuerdo No. 15-2009, del 15 de abril de 2009, se aprobó el Reglamento de la Ley de Protección al Consumidor que, entre otras cuestiones, desarrolla los medios de defensa que se pueden hacer valer a través de las Asociaciones de Consumidores, así como el procedimiento de arbitraje y los mecanismos de control contra las cláusulas abusivas. Sin embargo, no se considera a los consumidores en línea.

#### c) Protección de datos personales

La Constitución de la República de Honduras consagra el derecho al honor, a la intimidad personal, familiar y a la propia imagen, así como a la inviolabilidad y a la privacidad de las comunicaciones, e incorpora la garantía del Hábeas Data. Por su parte, la Ley de Transparencia y Acceso a la Información Pública establece los mecanismos para garantizar la protección, clasificación y seguridad de la información pública y el respeto a las restricciones de acceso en los casos de información reservada, información confidencial entregada por particulares y datos personales confidenciales.

Asimismo, regula el tratamiento de los datos personales y los distingue de los datos personales confidenciales, regula la garantía del Hábeas Data y prohíbe obligar a cualquier persona a proporcionar datos personales susceptibles de ocasionar discriminación o causar daños o riesgos patrimoniales o morales. También ordena la protección de los datos

personales. La Ley sanciona a quien se negare a proporcionar los datos personales, a su legítimo titular, sus sucesores o a una autoridad competente. También sanciona a quien recoja, capte, transmita o divulgue datos personales, o se niegue a rectificarlos, actualizarlos o a eliminar información falsa en los datos personales confidenciales contenidos en cualquier archivo, registro o base de datos de las Instituciones Obligadas. Las infracciones son sancionadas con independencia de la responsabilidad civil y/o penal que se pueda derivar.

#### d) Propiedad industrial e intelectual

En materia de propiedad intelectual, la Constitución de Honduras reconoce que todo autor, inventor, productor o comerciante gozará de la propiedad exclusiva de su obra, invención, marca o nombre comercial, con arreglo a la Ley.

Por su parte, la Ley del Derecho de Autor y de los Derechos Conexos, Decreto N° 4-99, protege a los autores de obras literarias, artísticas y de programación, así como a los artistas-intérpretes o ejecutantes, productores de fonogramas y organismos de radiodifusión. Los programas de computadoras son considerados como una obra literaria o artística. La Ley reconoce dentro de los derechos patrimoniales la facultad de realizar o autorizar el acceso público a bases de datos de ordenadores por medio de telecomunicaciones.

La Ley de la Propiedad Industrial, por Decreto N° 12-99, establece que los programas de computación considerados de manera aislada no son invenciones, razón por la cual no son susceptibles de patente.

En el ámbito internacional, Honduras ha ratificado

- el Convenio de París para la Protección de la Propiedad Industrial;
- la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes,
- los productores de fonogramas y los organismos de radiodifusión (Convención de Roma);
- el Convenio para la protección de los productores de fonogramas;
- el Convenio de Berna para la Protección de las Obras Literarias y Artísticas;
- el Tratado de Cooperación en materia de Patentes (PCT);
- los Tratados de la OMPI sobre Derecho de Autor (WCT) y sobre Interpretación o Ejecución y Fonogramas (WPPT);
- el Tratado de Beijing sobre Interpretaciones y Ejecuciones Audiovisuales (2012);

- el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), administrado por la Organización Mundial del Comercio (OMC), y
- el Convenio Centroamericano para la Protección de la Propiedad Industrial y el CAFTA-RD.

#### e) Nombres de dominio

La Red de Desarrollo Sostenible de Honduras (NIC Honduras ([www.nic.hn](http://www.nic.hn))) es la entidad encargada de administrar el dominio de nivel superior .hn, y ha incorporado en su Política de solución de controversias y su Reglamento, los principios de la Política uniforme de solución de controversias en materia de nombres de dominio de la ICANN.

La Ley de Propiedad Industrial considera que un signo distintivo se usa en el comercio cuando se adopta como nombre de dominio, dirección de correo electrónico, nombre o designación en medios electrónicos y otros similares empleados en los medios de comunicación electrónica o en el comercio electrónico.

#### f) Delitos Informáticos y Seguridad de la Información

En el ámbito de los delitos informáticos, el Código Penal castiga la interceptación de comunicaciones, incluyendo las cursadas a través de soportes electrónicos o computadoras. Igualmente castiga a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos, contenidos en redes, soportes o sistemas informáticos. También sanciona a quien cause daños a los medios o vías de comunicación.

Asimismo, castiga a quien destruya, oculte o falsifique libros de contabilidad, libros sociales, documentos legales, certificaciones, constancias, identidad personal, datos, registros, estados financieros, documentos cuyo soporte sea magnético o electrónico u otra información de una persona natural o jurídica, con el propósito de obtener, mantener o extender una facilidad crediticia o de capital de una institución supervisada, o con el propósito de encubrir, distorsionar o modificar maliciosamente operaciones activas o pasivas, obligaciones directas o contingentes, la iliquidez, la insolvencia, u otras situaciones fácticas que deban ser objeto de registro contable u otro tipo de registro.

La Ley impone pena privativa de la libertad a quien acceda ilegalmente a los sistemas de procesamiento de datos de las instituciones supervisadas, para alterar, borrar, dañar o sustraer registros, archivos u otra información de la institución o de sus clientes,

en beneficio propio o ajeno. Castiga de igual forma a quienes bajo cualquier procedimiento ingresen o utilicen indebidamente la base de datos de una institución supervisada para sustraer dinero mediante transferencias electrónicas de una cuenta a otra en la misma institución o en otra.

En materia de seguridad de la información, la Ley de Propiedad ordena que el soporte físico de los actos, contratos o documentos autorizados o certificados por notario deben incluir medios que eviten el fraude y que permitan verificar las declaraciones de las partes, tales como códigos de barras encriptados, uso de huellas digitales para verificar la identidad de los comparecientes y otros que los avances tecnológicos permitan. La Ley castiga con multa a quien: i) adultere los datos contenidos en los asientos de certificados, inscripciones y registros; ii) incumpla con las normas de seguridad de archivos y medios digitales; iii) ingrese sin autorización a archivos o bases de datos electrónicas; iv) sustraiga o copie sin autorización aplicaciones y tecnologías informáticas, e v) introduzca sin autorización software.

#### g) Iniciativas de Ley y retos

Entre los retos más relevantes que enfrenta Honduras se encuentra la aprobación de las distintas iniciativas de Ley previstas en la Agenda Digital de Honduras 2014, entre ellas, el proyecto de Ley sobre Comercio Electrónico, del 14 de agosto de 2014, el anteproyecto de Ley sobre Protección de Datos Personales y Acción de Hábeas Data de Honduras, de enero de 2014, así como el anteproyecto para la adopción del Convenio del Consejo de Europa sobre la Ciberdelincuencia. También está pendiente la redacción del Reglamento de la Ley de Firma Electrónica y la ampliación del contenido de la Ley de Protección al Consumidor para proteger a los consumidores en línea. La constitución de un CERT o CSIRT nacional es también una tarea pendiente.

## MÉXICO

Con la Reforma Constitucional del 11 de junio de 2013, se reconocieron como derechos fundamentales el acceso a las TIC, entre otros, el acceso a Internet de banda ancha, y se plantearon en el marco de la Estrategia Digital Nacional y las metas del Plan Nacional de Desarrollo 2013-2018, el facilitar el desarrollo de un ecosistema de la economía digital, lo cual deja en claro el compromiso del Gobierno Federal para promover el comercio electrónico.

En México no existe una ley especial que regule el comercio electrónico, sin embargo, diversas leyes

de carácter civil, mercantil, administrativo y fiscal han sido objeto de reformas para permitir el uso de mensajes de datos y medios electrónicos (particularmente de firmas electrónicas, firmas electrónicas avanzadas y certificados digitales emitidos por prestadores de servicios de certificación gubernamentales y/o privados, a efectos de reconocer su validez jurídica para la contratación entre particulares), sean empresas o consumidores, o con entidades de la Administración Pública.

#### a) Transacciones electrónicas / Firmas electrónicas

En el ámbito civil, el Código Civil Federal reconoce la posibilidad de manifestar la voluntad de las partes a través de medios remotos y reconoce la equivalencia funcional entre la firma autógrafa y la firma electrónica. Por su parte, el Código Federal de Procedimientos Civiles reconoce el valor probatorio de los mensajes de datos y establece las reglas para determinar su valor probatorio.

Por lo que se refiere al ámbito mercantil, el Código de Comercio incorpora un capítulo especial para el comercio electrónico, adoptando buena parte del contenido de las Leyes Modelo de la CNUDMI sobre Comercio Electrónico y las Firmas Electrónicas, y regula, entre otros temas, la firma electrónica, la firma electrónica avanzada y la prestación de servicios de certificación, así como la admisibilidad de los mensajes de datos como prueba en juicio. En el Reglamento del Código de Comercio en materia de Prestadores de Servicios de Certificación, las Reglas Generales y el Acuerdo que las modifica se desarrollan con mayor detalle los requerimientos técnicos, administrativos y legales de su operación para robustecer el marco legal a las que deberán sujetarse los prestadores de servicios de certificación

De igual forma, se han instrumentado medidas para la operación del Registro Público del Comercio a través de medios electrónicos, a nivel de ley y reglamento, incorporándose, entre otras medidas, aquellas que regulan la sección del Registro Único de Garantías Mobiliarias que opera a través del sitio web (<http://www.rug.gob.mx>), que permite, entre otras cuestiones, que las instituciones financieras o los acreedores puedan inscribir los actos por virtud de los cuales se constituyen, transmiten, modifican o cancelan garantías mobiliarias, así como cualesquier privilegio especial o derecho de retención sobre bienes muebles.

La Ley de Instituciones de Crédito también faculta a las instituciones financieras para prestar sus servicios a través de medios electrónicos. Con respecto a las transacciones de banca en línea y de banca móvil,

las “Disposiciones de carácter general aplicables a instituciones de crédito”, emitidas por la Comisión Nacional Bancaria y de Valores, conocidas como “Circular Única de Bancos”, han dado sustento normativo a las operaciones con medios electrónicos de pago, incluyendo los servicios de banca móvil.

En el ámbito administrativo, la Ley Federal de Procedimiento Administrativo, la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y la Ley de Obras Públicas y Servicios Relacionadas con las Mismas reconocen el uso de medios electrónicos para interactuar con la Administración Pública Federal a través de sistemas que utilizan firmas electrónicas avanzadas, amparadas con certificados digitales, en procesos administrativos y procesos de contratación gubernamental.

Con la Ley de Firma Electrónica Avanzada y su Reglamento, se robustece el marco legal para las comunicaciones en línea que utilizan firmas y certificados digitales entre las entidades de la Administración Pública en sus tres niveles de gobierno: federal, estatal y municipal.

Asimismo, el Ejecutivo Federal expidió el Acuerdo que tiene por objeto emitir las políticas y disposiciones para la Estrategia Digital Nacional en materia de tecnologías de la información y comunicaciones y seguridad de la información, así como establecer el Manual Administrativo de Aplicación General en dichas materias, en virtud de los cuales se promueve, entre otros temas, el uso de soluciones de cómputo en la nube por parte de las entidades de la Administración Pública Federal y se fomenta las prácticas en materia de seguridad de la información.

En cuanto a las leyes fiscales, el Código Fiscal de la Federación, la Ley Aduanera y la Ley del Seguro Social facultan a las autoridades tributarias para utilizar medios electrónicos en diversos trámites, procesos y documentos (incluyendo los comprobantes fiscales digitales). Las leyes en comento reconocen la equivalencia funcional de la firma autógrafa y la firma electrónica, y regulan también la utilización de firmas electrónicas avanzadas, amparadas por certificados digitales. El contenido de estas leyes también ha sido desarrollado con mayor detalle a través de la regulación administrativa emanada del Poder Ejecutivo Federal.

#### b) Protección al consumidor

Por su parte, la Ley Federal de Protección al Consumidor establece un capítulo especial que regula los derechos de los consumidores en las transacciones efectuadas a través del uso de medios electrónicos y

reconoce la utilización de los Códigos de Ética como mecanismos de autorregulación válidos, los cuales han permitido el desarrollo de esquemas de sellos de confianza acordes con las mejores prácticas internacionales, como el Sello de Confianza de la Asociación Mexicana de Internet (AMIPCI), que forma parte de Asia Pacific Trustmark Alliance, la cual opera en la región Asia-Pacífico en cumplimiento con el Marco de Privacidad del APEC.

El Sello de Confianza también busca ser instrumento eficiente para el cumplimiento normativo de las obligaciones en materia de protección de datos personales.

#### c) Protección de datos personales

Por lo que se refiere a la Protección de Datos Personales, la Constitución ha reconocido en su artículo 6º su carácter de derecho fundamental. Además de las leyes sectoriales, como la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, la Ley de Instituciones de Crédito y la Ley Federal de Protección al Consumidor establecen medidas para proteger a los titulares de datos personales.

Con la adopción de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento, se completó el régimen de protección en la materia en México, al incorporarse una ley general aplicable al tratamiento de datos personales efectuado por personas físicas y/o morales de carácter privado que recolecten y procesen datos personales, con independencia de su sector o industria, y se genera un sistema de protección alineado con los estándares internacionales, particularmente con el modelo europeo, Marco de Privacidad del APEC, teniendo en cuenta las particularidades del Tratado de Libre Comercio de América del Norte (TLCAN).

Asimismo, México se convirtió, en enero de 2013, en la segunda economía en formar parte del Sistema de normas transfronterizas sobre privacidad del APEC. La operación del Sistema se sustenta en la Ley Federal de Protección de Datos Personales, en su Reglamento y en los nuevos Parámetros de Autorregulación en materia de Datos Personales publicados en el Diario Oficial de la Federación (DOF), el 29 de mayo de 2014.

#### d) Propiedad industrial e intelectual

Por su parte, en el ámbito de la propiedad intelectual, México ha incorporado en su Ley Federal del Derecho de Autor, la protección a los programas de cómputo, así como la figura de la reserva de derechos al uso exclusivo de títulos para su difusión periódica en Internet. De igual forma, ha incluido en el Código

Penal Federal diversos delitos vinculados con la reproducción y comercialización a gran escala de obras protegidas por derechos de autor, sin la correspondiente autorización de su titular.

Adicionalmente, México ha suscrito:

- el Tratado de Beijing sobre Interpretaciones y Ejecuciones Audiovisuales (2012);
- los Tratados de la OMPI sobre Derecho de Autor (WCT) y sobre Interpretación o Ejecución y Fonogramas (WPPT);
- el Convenio de Berna para la Protección de las Obras Literarias y Artísticas;
- el Convenio de Ginebra para la protección de los productores de fonogramas contra la reproducción no autorizada de sus fonogramas;
- la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma);
- el Convenio de Bruselas sobre la distribución de señales portadoras de programas transmitidas por satélite;
- los Tratados de Internet (WCT y WPPT), y
- el ADPIC, administrado por la OMC.

#### e) Nombres de dominio

En materia de nombres de dominio, el NIC México ha adoptado dentro de sus políticas de resolución de controversias en materia de nombres de dominio el procedimiento arbitral previsto en la Política uniforme de solución de controversias de la ICANN, y reconoce dentro de los proveedores de servicios de arbitraje al Centro de Arbitraje y Mediación de la OMPI.

#### f) Delitos Informáticos y Seguridad de la Información

En cuanto al ámbito penal, el Código Penal Federal ha tipificado los delitos relacionados con la interceptación de comunicaciones, el acceso ilícito a los sistemas de cómputo y el daño informático. Por su parte, la Ley de Instituciones de Crédito ha incluido diversos delitos relacionados con el fraude a través de medios electrónicos.

En virtud de la Ley Federal de Telecomunicaciones y Radiodifusión, se han ampliado las facultades de las autoridades encargadas de la procuración de justicia y de las instancias de seguridad al establecer diversas obligaciones para los prestadores de servicios de telecomunicaciones, sean concesionarios, autorizados o proveedores de servicios de aplicaciones y contenidos, para permitir a las autoridades el acceso a información en tiempo real sobre comunicaciones,

usuarios y dispositivos relacionados con la investigación de delitos.

Por otra parte, es importante señalar que, a la fecha, no se ha desarrollado un régimen legal que permita delimitar la responsabilidad de los Prestadores de Servicios de Internet, lo cual desincentiva el desarrollo de las plataformas tecnológicas y de las redes de acceso a Internet.

Con la entrada en vigor del Código Nacional de Procedimientos Penales, se espera lograr un sistema de cooperación nacional eficiente que unifique los distintos ordenamientos locales. A nivel federal, el Código deberá entrar en vigor antes del 18 de junio de 2016 y, a nivel estatal, no se han determinado aún los tiempos que tomará este proceso, sin embargo, se espera que con el Código se eliminen las contradicciones procesales existentes entre el marco federal y el marco previsto para cada uno de los 32 estados.

México forma parte de la COMJIB y ha suscrito el Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia, así como la Recomendación relativa a la Tipificación y Sanción de la Ciberdelincuencia. También ha sido invitado por el Consejo de Europa para adherirse al Convenio sobre la Ciberdelincuencia, sin que a la fecha se haya materializado su adhesión.

#### g) Iniciativas de Ley y retos

Actualmente se discuten en el Congreso de la Unión distintas iniciativas de reforma al Código Penal Federal y al Código Nacional de Procedimientos Penales, a efectos de incorporar en el derecho nacional las medidas sustantivas y procesales previstas en el Convenio del Consejo de Europa sobre la Ciberdelincuencia y homologar la normativa a nivel federal y en los estados. De igual forma, se encuentra en proceso de debate parlamentario una Ley General de Protección de Datos Personales, derivada del mandato constitucional en virtud del cual se reformó el Artículo 6º Constitucional, el 7 de febrero de 2014.

Los principales retos se centran en el despliegue de infraestructura para la conectividad y en la creación de capacidades para un mejor entendimiento y aprovechamiento de los aspectos legales de las TIC para promover el comercio electrónico.

## NICARAGUA

El Plan Nacional de Desarrollo Humano 2012-2016 establece entre sus metas el fortalecer el comercio electrónico, y el “Programa de Fortalecimiento a la Se-

guridad y Confianza del Uso del Comercio Electrónico en Nicaragua” del Ministerio de Fomento, Industria y Comercio (MIFIC) promueve el uso de la firma electrónica. Entre los principales instrumentos legales que habilitan el comercio electrónico se encuentra la Ley de Firma Electrónica (Ley N° 729), del 30 de agosto de 2010, reglamentada mediante Decreto Ejecutivo N° 57-2011, del 8 de noviembre de 2011.

#### a) Transacciones electrónicas / Firmas electrónicas

La Ley de Firma Electrónica incorpora las disposiciones de la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas, otorga y reconoce la eficacia y el valor jurídico de la firma electrónica y de los certificados digitales, así como de la información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, y regula a los proveedores de servicios de certificación. La Ley distingue la firma electrónica de la firma electrónica certificada, confiriéndoles diferentes efectos jurídicos y reconoce la equivalencia funcional de los documentos impresos respecto de los documentos consignados en mensajes de datos, así como de la firma manuscrita respecto de la firma electrónica certificada, amparada por un certificado expedido por un prestador de servicios acreditado.

También faculta a las autoridades del Estado de los distintos poderes para llevar a cabo trámites administrativos a través de medios electrónicos y a utilizar expedientes electrónicos y firmas digitales en sus actuaciones, sea entre sí o con los particulares.

En virtud del Reglamento de la Ley de Firma Electrónica, Decreto N° 57-2011, del 8 de noviembre de 2011, se faculta a la Dirección General de Tecnología del Ministerio de Hacienda y Crédito Público como ente rector del Proceso de Acreditación de Firma Electrónica y se detallan las facultades de la Autoridad Certificadora y las obligaciones y deberes de los Prestadores de Servicios de Certificación

En el ámbito financiero, la Ley General de Bancos, Instituciones Financieras No Bancarias y Grupos Financieros, del 30 de noviembre de 2005, autoriza a los bancos a incorporar sistemas computarizados y de microfilmación para la prestación de sus servicios. Los documentos reproducidos de esos sistemas tendrán pleno valor probatorio, siempre y cuando los mecanismos utilizados para su reproducción apliquen las resoluciones o reglamentos emitidos por la Superintendencia de Bancos y se encuentren debidamente firmados por funcionario autorizado.

La Resolución N° CD-SIBOIF-725-1-ABR26-2012, de fecha 26 de abril de 2012, normativa que regula las operaciones con dinero electrónico realizadas por instituciones financieras emitida por la Superintendencia de Bancos y de Otras Instituciones Financieras, merece especial mención en el ámbito de las transacciones de banca móvil.

Respecto a las transacciones gubernamentales en línea, la Ley N° 691 sobre Simplificación de Trámites y Servicios de la Administración Pública, del 3 de agosto de 2009, establece las bases y principios para simplificar y racionalizar los trámites y servicios a fin de garantizar que las instituciones del Estado actúen de conformidad con las normas de economía, transparencia, celeridad, eficacia y espíritu de servicio, logrando la pronta y efectiva solución a los problemas planteados por los usuarios. La Ley promueve la instrumentación de la Ventanilla Única de Trámites y/o Servicios, así como el uso de medios electrónicos para agilizar las gestiones.

Por su parte, la Ley de Contrataciones Administrativas del Sector Público (Ley N° 737), del 8 y 9 de noviembre de 2010, regula el régimen jurídico sustantivo y procesal para la preparación, adjudicación, ejecución y extinción de las adquisiciones celebradas por las entidades del Sector Público. La Ley es aplicable también a las empresas públicas y a las entidades financieras en cuanto a aquellas adquisiciones relacionadas con la actividad administrativa. Además, faculta a la Dirección General de Contrataciones del Estado como el Órgano Rector del Sistema de Administración de Contrataciones del Sector Público "SISCAE", a efectos de supervisar la actuación de las Entidades Contratantes, debiendo comunicar a la Contraloría General de la República las prácticas negligentes o corruptas detectadas en el actuar de los funcionarios públicos. Asimismo, se faculta a la citada Dirección General para sancionar a proveedores/contratistas que contravengan la Ley, su Reglamento General y demás disposiciones administrativas en materia de adquisiciones. La Ley fomenta el desarrollo de las micro, pequeñas y medianas empresas, incentivando su participación en los procesos de contratación.

Por su parte, el Reglamento General de la Ley de Contrataciones Administrativas del Sector Público (Ley N° 737), del 15 y 16 de diciembre de 2010, amplía las facultades de la Dirección General de Contrataciones del Estado como Órgano Rector a cargo del Sistema de Administración de Contrataciones del Sector Público, otorgándole la potestad de establecer a través de guías, los mecanismos y formalidades para el uso de formatos electrónicos o manuales para el regis-

tro de la información de los contratantes. Asimismo, establece el Registro de Proveedores en línea, operado por la Dirección General de Contrataciones del Estado, en el que se pueden inscribir todas las personas, naturales y jurídicas, nacionales y extranjeras, que no tengan causal de prohibición para contratar con el Estado. En el portal ([www.nicaraguacompra.gob.ni](http://www.nicaraguacompra.gob.ni)) se publican el procedimiento y los formularios a utilizar para el alta y la baja a las entidades, las áreas que requieren de las adquisiciones y los funcionarios relacionados.

Por lo que se refiere al ámbito aduanero, cabe destacar que Nicaragua ha adoptado el CAUCA, el RECAUCA y el CAFTA-RD.

#### b) Protección al consumidor

La Ley de Protección de los Derechos de las Personas Consumidoras y Usuarias (Ley N° 842), del 11 de julio de 2013 (Ley de Protección de los Consumidores), incorpora los derechos fundamentales de los consumidores previstos en la Resolución 39/248 sobre las Directrices de las Naciones Unidas para la Protección al Consumidor, entre ellos, el derecho de los consumidores a la información y productos seguros. Asimismo, incorpora el derecho de retracto en las ventas fuera del establecimiento comercial o a distancia, el derecho a la privacidad y el derecho a la protección real y efectiva en las transacciones electrónicas. También incorpora dentro de las cláusulas abusivas de los contratos de servicios financieros aquellas que deslindan a las instituciones financieras de responsabilidad en caso de virus, programas fraudulentos o exposición no autorizada o ilícita de sus servicios vía medios electrónicos.

La Ley también regula la contratación de productos y servicios financieros por medios electrónicos y les confiere el mismo valor probatorio y efecto legal que a los contratos celebrados de manera presencial. Asimismo, reconoce las transacciones por medios electrónicos y determina la información que se debe suministrar a los consumidores previo a la celebración de la transacción en línea, incluyendo lo referente a su domicilio físico, dirección electrónica y demás medios para presentar reclamos y aclaraciones, así como información sobre los bienes y servicios, evitando prácticas comerciales engañosas que induzcan al fraude o a confusión. También obliga a los proveedores a utilizar sistemas tecnológicos y elementos técnicos confiables para brindar seguridad y confianza a la información transmitida y proporcionada por los consumidores en las transacciones electrónicas, así como a informar sobre estas medidas a los consumidores.

En cuanto a la compra de bienes y servicios en territorio nacional por medio de transacciones electrónicas, se obliga al proveedor a entregar factura por vía electrónica y a mantener el registro de los pagos electrónicos, así como a enviarle el contrato de compraventa con toda la información relacionada con los términos y condiciones, costos, y garantías.

### c) Protección de datos personales

En materia de protección de datos personales, la Constitución Política de la República de Nicaragua, del 19 de noviembre de 1986, consagra el derecho de toda persona a la vida privada, a la inviolabilidad del domicilio, de la correspondencia y comunicaciones de todo tipo, así como a conocer toda información que sobre ella hayan registrado las autoridades estatales, y el derecho de saber por qué y con qué finalidad poseen esa información.

En ese sentido, la Ley de Acceso a la Información Pública (Ley No. 621), del 22 de junio de 2007, incorpora el recurso de Hábeas Data para tutelar los datos personales privados asentados en archivos, registros, bancos de datos u otros medios técnicos, sean estos públicos o privados, cuya publicidad constituya una invasión a la privacidad personal familiar que tenga relevancia con respecto a datos sensibles de las personas, su vida íntima, incluyendo sus asuntos familiares, que se encuentren en poder de los sujetos obligados de la Administración Pública. El Hábeas Data garantiza el acceso de toda persona a la información que puede tener cualquier entidad pública sobre ella, así como el derecho a saber por qué y con qué finalidad tienen esa información.

La Ley de Protección de Datos Personales (Ley N° 787), del 29 de marzo de 2012, es conforme con las Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana emitidas por la Red Iberoamericana de Protección de Datos Personales. La Ley protege los datos personales, automatizados o no, de toda persona natural o jurídica, y el manejo de esta información en ficheros públicos o privados, a efectos de garantizar el derecho a la privacidad de las personas y el derecho a la autodeterminación informativa. La Dirección de Protección de Datos Personales, adscrita al Ministerio de Hacienda y Crédito Público, es la entidad encargada de supervisar la aplicación de la Ley que clasifica los datos personales en datos personales simples, datos personales informáticos, datos personales sensibles, datos personales relativos a la salud y datos personales comerciales. También establece la obligación de registrar los ficheros con datos personales ante la Dirección de Protección de Datos Personales y prohíbe

la transferencia de datos personales a países u organismos internacionales que no proporcionen niveles de seguridad y protección adecuados.

Las personas y entidades públicas o privadas que hacen uso, almacenan o transfieren información privada de sus clientes o usuarios se encuentran obligadas a: i) que el uso de la información sea adecuado, proporcional y necesario en relación al ámbito y las finalidades para el que se colecta; ii) obtener consentimiento del titular para la entrega de los datos; iii) usar los datos para los fines que motivaron su obtención, y iv) a adoptar las medidas técnicas y organizativas para garantizar la seguridad y confidencialidad de los datos personales.

La violación a la Ley se castiga con sanciones administrativas y penales. La Ley otorga al titular de los datos el derecho a solicitar información a la Dirección de Protección de Datos Personales relativa a la existencia de archivos sobre él en ficheros de datos personales, sus finalidades y la identidad de sus responsables. También le faculta para solicitar al responsable rectificar, modificar, suprimir, complementar, incluir, actualizar o cancelar sus datos personales. La Ley las clasifica en infracciones leves y graves y establece sanciones administrativas, con independencia de la responsabilidad civil y penal que pueda derivar.

Mediante el Decreto N° 36-2012, del 17 de octubre de 2012, se aprueba el Reglamento de la Ley de Protección de Datos Personales (Ley N° 787), en virtud del cual se desarrollan con detalle diversos aspectos de la Ley como los referentes a los derechos de acceso, rectificación, cancelación y oposición, al igual que los relacionados con las medidas de seguridad y los procedimientos de inspección y los sancionatorios.

### d) Propiedad industrial e intelectual

En cuanto a los derechos de propiedad intelectual, la Constitución de Nicaragua reconoce que la creación artística y cultural es libre e irrestricta. Asimismo, determina que los trabajadores de la cultura tienen plena libertad de elegir formas y modos de expresión, teniendo el Estado el deber de facilitarles los medios necesarios para crear y difundir sus obras y para proteger sus derechos de autor.

La Ley de Derecho de Autor y de los Derechos Conexos (Ley N° 312), del 6 de julio de 1999, reformada por última ocasión el 16 de marzo de 2006, protege a los programas de cómputo en los mismos términos que a las obras literarias. La protección se amplía a la documentación técnica y a sus manuales de uso. También protege a las bases de datos, restringiendo de la autorización para la reproducción para uso personal a

la reproducción de la totalidad o partes importantes de bases de datos en forma numérica. La Ley tipifica el delito de evasión de medidas tecnológicas para permitir el acceso no autorizado a una obra, la interpretación o ejecución de fonogramas protegidos u otra materia objeto de protección.

En cuanto a la propiedad industrial, la Ley de Patentes de Invención, Modelo de Utilidad y Diseños Industriales (Ley N° 354), del 22 y 25 de septiembre de 2000, en su artículo 6° no considera como invenciones susceptibles de patente a los métodos matemáticos ni a los programas de ordenador considerados de manera aislada. Por su parte, la Ley de Marcas y Otros Signos Distintivos (Ley N° 380), del 16 de abril de 2001, establece los requisitos y términos en que se protegen las marcas, los nombres de dominio, los nombres comerciales, las denominaciones de origen y otros signos distintivos.

En el ámbito internacional de los derechos de propiedad intelectual, Nicaragua ha ratificado

- los Tratados de la OMPI sobre Derecho de Autor (WCT) y sobre Interpretación o Ejecución y Fonogramas (WPPT);
- el Tratado de Beijing sobre Interpretaciones y Ejecuciones Audiovisuales (2012);
- el Protocolo al Convenio Centroamericano para la Protección de la Propiedad Industrial;
- el Tratado de Libre Comercio entre la República Dominicana, Centroamérica y Estados Unidos (CAFTA-RD);
- el Convenio de París para la Protección de la Propiedad Industrial (1883);
- el Convenio de Berna para la Protección de las Obras Literarias y Artísticas;
- el Convenio de Ginebra para la protección de los productores de fonogramas contra la reproducción no autorizada de sus fonogramas;
- la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma);
- el Convenio de Bruselas sobre la distribución de señales portadoras de programas transmitidas por satélite, y
- el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), administrado por la Organización Mundial del Comercio (OMC).

#### e) Nombres de dominio

En materia de nombres de dominio y, además de lo previsto por la Ley de Marcas y Otros Signos Distintivos (Ley N° 380), el NIC-NI (Nicaragua) (<http://nic.ni>) es la entidad que administra los nombres de dominio de nivel superior de código de país .ni. El NIC-Nicaragua, en su carácter de autoridad registradora, ha incorporado la Política uniforme de solución de controversias en materia de nombres de dominio de la ICANN, motivo por el cual se ajusta a las mejores prácticas internacionales y reconoce dentro de los proveedores de servicios de solución de controversias al Centro de Arbitraje y de Mediación de la OMPI.

Cabe mencionar que la Ley de Marcas y Otros Signos Distintivos (Ley N° 380) reconoce dentro de los casos de uso de marca al uso del signo distintivo como nombre de dominio, dirección de correo electrónico, nombre o designación en medios electrónicos y otros similares empleados en los medios de comunicación electrónica o en el comercio electrónico.

#### f) Delitos Informáticos y Seguridad de la Información

La Ley 641 del Código Penal, del 13 de noviembre de 2007, castiga a quien ilícitamente abra, intercepte o por cualquier otro medio se entere del contenido de una carta, un pliego cerrado o un despacho telegráfico, telemático, electrónico o de otra naturaleza que no le esté dirigido. También castiga a quien sin autorización de ley promueva, facilite, autorice, financie, cree o comercialice un banco de datos o un registro informático con datos que puedan afectar a las personas naturales o jurídicas.

De igual forma, castiga a quien, sin la debida autorización, utilice registros informáticos de otro, o ingrese por cualquier medio a su banco de datos o archivos electrónicos. También sanciona a la persona que se apodere por cualquier medio de información, de datos, documentos escritos o electrónicos, registros informáticos u otros medios u objetos que contengan un secreto empresarial, sin autorización.

#### g) Iniciativas de Ley y retos

Entre los principales retos que enfrenta Nicaragua se encuentra el tema de la ciberseguridad y el establecimiento de un CSIRT Nacional, al igual que la emisión de leyes que la incentiven. Entre las principales iniciativas de Ley que se encuentran en proceso de revisión en la Asamblea Nacional está el Anteproyecto de Ley de Gobierno Electrónico de Nicaragua y el Anteproyecto de Ley Especial de Protección contra los Delitos Informáticos.

## PANAMÁ

El ordenamiento de mayor relevancia para el desarrollo del comercio electrónico en Panamá es la Ley N° 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 (Ley N° 51) que se detallan a continuación.

### a) Transacciones electrónicas / Firmas electrónicas

El objeto de la Ley N° 51 consiste en establecer el marco regulador para la creación, la utilización y el almacenamiento de documentos electrónicos y firmas electrónicas, así como el proceso de registro y la fiscalización de los prestadores de servicios de almacenamiento tecnológico de documentos y de certificación de firmas electrónicas en Panamá.

La misma incorpora diversos elementos de las Leyes Modelo de la CNUDMI sobre Comercio Electrónico y las Firmas Electrónicas, así como de las Directivas Europeas sobre Comercio Electrónico, Firmas Electrónicas y Ventas Directas a Distancia. Regula diversos temas vinculados con las transacciones electrónicas entre particulares y con entidades de la Administración Pública.

Además, la Ley N° 51 establece el marco regulador de diversos actos de comercio realizados vía Internet, principalmente en lo referente a la información previa y posterior a la celebración de contratos electrónicos y a las condiciones relativas a la validez y eficacia de dichos contratos. También determina las obligaciones y responsabilidades de los prestadores de servicios comerciales a través de Internet, incluidos los que actúan como intermediarios en la transmisión de contenidos, alojamiento y copia temporal, así como las limitantes de responsabilidad; el intercambio de información y documentación comercial por vía electrónica, incluidas las ofertas, las promociones y los concursos, y el régimen sancionador aplicable a los prestadores de servicios comerciales a través de medios electrónicos.

La Ley N° 51 reconoce la equivalencia funcional de los documentos impresos con firma autógrafa respecto de los documentos electrónicos con firma electrónica calificada, respaldada por un certificado digital emitido por un prestador de servicios de certificación debidamente acreditado ante el Registro Público. También reconoce los certificados digitales extranjeros emitidos por autoridades competentes de otros países, siempre que cumplan con los estándares requeridos por el Registro Público.

Asimismo, reconoce que los documentos electrónicos serán admisibles como medios de prueba y tendrán la misma fuerza probatoria otorgada a los documentos y, en todo caso, al valorar la fuerza probatoria de un documento electrónico se tendrá presente la confiabilidad de la forma en la que se haya generado, archivado o comunicado, así como la confiabilidad de la forma en la que se haya conservado la integridad de la información.

La Ley N° 51 fue modificada por la Ley N° 82, del 9 de noviembre de 2012, a efectos de trasladar las competencias que en materia de firma electrónica tenía la Dirección General de Comercio Electrónico del Ministerio de Comercio e Industrias a la Dirección Nacional de Firma Electrónica del Registro Público de Panamá. Introdujo el Capítulo II, "Reglas de Comunicación Electrónica", que dan mayor sustento al tema de la formación de contratos a través de medios electrónicos, incorporando distintas medidas previstas en la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales, suscrita por Panamá, y que se encuentra en proceso de ratificación ante la Asamblea Nacional.

En el ámbito financiero, destaca el Acuerdo N° 6 de 2011, promulgado por la Superintendencia de Bancos de la República de Panamá, que establece lineamientos sobre la banca electrónica y la gestión de riesgos relacionados, obligando a las instituciones bancarias de Panamá a modernizar sus sistemas electrónicos de prestación de servicios.

Por lo que se refiere al contexto gubernamental, la Ley N° 51 faculta al Estado para hacer uso del almacenamiento tecnológico de documentos en su ámbito interno y en su relación con los particulares. Asimismo, mediante la Ley N° 83, del 9 de noviembre de 2012, se establecen las normas que rigen el uso de medios electrónicos para los trámites gubernamentales previamente sustentados en el Decreto Ejecutivo N° 928, del 21 de septiembre de 2010, denominado "Panamá Sin Papel".

Por su parte, el Decreto Ejecutivo N° 847, del 20 de octubre de 2014, establece el Sistema de Inscripción Electrónico Registral (SIR) basado en la técnica de Folio Electrónico, incorporando el uso de la firma electrónica reconocida para todas las operaciones y procedimientos registrales que deban efectuarse en el Registro Público de Panamá, a fin de robustecer los atributos de seguridad, es decir, autenticidad, integridad y no repudio, de los documentos en materia de operaciones registrales.

Por lo que se refiere al ámbito aduanal, destaca el Decreto Ley N° 1, del 13 de febrero de 2008, por el que se crea la Autoridad Nacional de Aduanas y se establecen diversas disposiciones en virtud de las cuales se acepta la utilización de soportes electrónicos para los trámites aduaneros.

En materia fiscal, la Ley N° 51 de 2008 establece la legalidad de la factura electrónica y reconoce la validez tributaria de las operaciones comerciales efectuadas a través de medios electrónicos. El Código Fiscal y la Resolución N° 201-2969, del 15 de agosto de 2007, emitida por la Dirección General de Ingresos del Ministerio de Economía y Finanzas, autorizan la presentación de declaraciones juradas a través de medios electrónicos.

#### b) Protección al consumidor

Por mandato constitucional, toda persona tiene derecho a obtener bienes y servicios de calidad, información veraz, clara y suficiente sobre las características y el contenido de los bienes y servicios que adquiere, así como a la libertad de elección y a condiciones de trato equitativo y digno.

Por su parte, la Ley N° 51 incluye diversas medidas vinculadas con la protección a los consumidores que lleven a cabo operaciones de comercio electrónico y con la responsabilidad de los prestadores de servicios comerciales a través de Internet, incluidos a los prestadores de servicios de intermediación. La Ley establece medidas para limitar las comunicaciones comerciales no solicitadas incluyendo las cursadas vía Internet. También autoriza el uso de sellos de confianza para promover el uso de Internet como medio seguro para ofrecer y obtener bienes y servicios comerciales.

#### c) Protección de datos personales

La Constitución de Panamá de 1972, reformada el 15 de noviembre de 2004, consagra la inviolabilidad de las comunicaciones privadas que no pueden ser interceptadas o grabadas, sino por mandato de autoridad judicial. El incumplimiento de lo anterior impide la utilización de sus resultados como pruebas, sin perjuicio de las responsabilidades penales en que incurran los autores. También reconoce el derecho de toda persona para acceder a la información personal contenida en bases de datos o registros públicos y privados, y a requerir su rectificación y protección, así como su supresión. Tal información solo puede ser recogida para fines específicos, mediante el consentimiento de su titular o por disposición de autoridad competente con fundamento en lo previsto en la Ley.

Asimismo, la Constitución reconoce el derecho de promover la acción de Hábeas Data para garantizar el derecho de acceso a la información personal recabada en bancos de datos o registros oficiales o particulares, cuando estos últimos traten de empresas que prestan un servicio al público o se dediquen a suministrar información. Mediante la acción de Hábeas Data se puede solicitar que se corrija, actualice, rectifique, suprima o se mantenga en confidencialidad la información o los datos que tengan carácter personal.

Por su parte, la Ley N° 51 crea un régimen especial para garantizar la inviolabilidad de la información depositada en bancos de datos como respaldo de operaciones que se realicen en países o jurisdicciones extranjeras por empresas privadas o públicas, incluyendo organismos estatales e internacionales. Asimismo, la Ley N° 24 de 2002, del 22 de mayo de 2002, modificada y adicionada por la Ley N° 14 de 2006, del 18 de mayo de 2006, desarrolla diversas medidas relacionadas con el manejo de la información sobre el historial crediticio de los consumidores.

#### d) Propiedad industrial e intelectual

Por lo que se refiere a la normativa en materia de propiedad industrial, es preciso señalar que después de la ratificación del Tratado de Promoción Comercial entre la República de Panamá y los Estados Unidos de Norteamérica, la Ley N° 35, del 10 de mayo de 1996, fue modificada en virtud de la Ley N° 61, del 5 de octubre de 2012, y se incorpora la utilización de medios electrónicos para la presentación de solicitudes de registros de marcas, patentes, modelos industriales y demás, ante la Dirección General del Registro de la Propiedad Industrial (DIGERPI).

Adicionalmente, Panamá ha suscrito:

- los Tratados Internacionales administrados por la Organización Mundial de la Propiedad Intelectual (OMPI), incluyendo el Tratado de Cooperación en Materia de Patentes (PCT, por sus siglas en inglés) y el Tratado sobre el Derecho de Marcas (TLT), y
- el Tratado de la OMPI sobre Derecho de Autor (WCT) y el Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas (WPPT).
- También ha ratificado
- el Protocolo al Convenio Centroamericano para la Protección de la Propiedad Industrial;
- el Tratado de Libre Comercio entre la República Dominicana, Centroamérica y Estados Unidos (CAFTA-RD), y

- el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), administrado por la Organización Mundial del Comercio (OMC).

En materia de derecho de autor y derechos conexos, mediante la Ley N° 64, del 10 de octubre de 2012, se deroga la Ley N° 15, del 8 de agosto de 1994, a efectos de adecuar sus normas al “entorno digital” de la “Sociedad de la Información”. Se amplía el alcance de la Ley para regular, además de las obras ya protegidas, incluyendo los programas de ordenador (software) y las bases de datos, conceptos como la información sobre la gestión de derechos y las medidas tecnológicas efectivas de autotutela. En cuanto a los derechos conexos de artistas, intérpretes, ejecutantes y organismos de radiodifusión, igualmente se reconocen los conceptos de fonogramas y videogramas, y se reconoce el derecho de comunicación pública por cualquier medio. La Ley se encuentra en proceso de reglamentación.

#### e) Nombres de dominio

En materia de nombres de dominio, el NIC-Panamá (<http://nic.pa>), centro adscrito a la Universidad Tecnológica de Panamá (UTP), es la entidad que administra los nombres de dominio de nivel superior de código de país “.pa” y, en su carácter de autoridad registradora, ha incorporado la Política uniforme de solución de controversias en materia de nombres de dominio de la ICANN, razón por la cual se adapta a las mejores prácticas internacionales y reconoce dentro de los proveedores de servicios de solución de controversias al Centro de Arbitraje y Mediación de la OMPI.

#### f) Delitos Informáticos y Seguridad de la Información

La Ley N° 51 tipifica como delito la alteración o adulteración de los documentos almacenados tecnológicamente, así como la revelación indebida de la información tecnológica almacenada. Por su parte, la Ley N° 14 del Código Penal tipifica diversos ilícitos vinculados con el acceso ilícito a los sistemas informáticos, así como con la interceptación de comunicaciones electrónicas, con agravante si se cometen contra datos contenidos en bases de datos o sistema informático de: i) oficinas públicas; ii) instituciones públicas, privadas o mixtas que prestan un servicio público, y iii) bancos, aseguradoras y demás instituciones financieras y bursátiles. También sanciona la divulgación ilícita de secretos industriales y la reproducción no autorizada de obras protegidas por los derechos de autor y los derechos conexos.

Mediante la Ley N° 79, del 22 de octubre de 2013, Panamá ratificó el Convenio del Consejo de Europa

sobre la Ciberdelincuencia. Asimismo, es preciso señalar que Panamá forma parte de la Conferencia de Ministros de Justicia de los Países Iberoamericanos (COMJIB).

En materia de seguridad de la información, la Autoridad Nacional para la Innovación Gubernamental (AIG) administra el CSIRT Panamá, Centro Nacional de Respuesta a Incidentes de Seguridad Cibernética de Panamá, creado en virtud del Decreto Ejecutivo N° 709 (2011), el cual coordina todas las actividades orientadas a prevenir y responder a los ataques cibernéticos dirigidos contra los sistemas informáticos gubernamentales y de infraestructuras críticas.

#### g) Iniciativas de Ley y retos

La Asamblea Nacional está discutiendo el proyecto de Ley sobre Delitos Informáticos (Ley N° 105), de fecha 16 de octubre de 2014, con lo que da cumplimiento a las obligaciones asumidas en virtud de la adhesión de Panamá al Convenio del Consejo de Europa sobre la Ciberdelincuencia.

De igual forma, la Dirección General de Comercio Electrónico del Ministerio de Comercio e Industrias está preparando un nuevo Decreto Ejecutivo que reglamentará la Ley N° 51 de 2008, conforme quedó modificada por la Ley N° 82 de 2012, así como los reglamentos en materia de almacenamiento tecnológico de documentos y comercio electrónico. Asimismo, se está trabajando en nuevos Decretos Ejecutivos para reglamentar la nueva legislación en materia de propiedad industrial y derecho de autor y derechos conexos.

La Autoridad Nacional para la Innovación Gubernamental se encuentra en proceso de consulta pública para la preparación de una Ley Integral de Protección de Datos Personales.

Entre los principales retos que enfrenta Panamá se encuentra el cierre de la brecha digital, para lo cual es preciso promover estrategias con el fin de facilitar el acceso de las micro y pequeñas empresas al comercio electrónico, e instrumentar esquemas de autorregulación, como los sellos de confianza. También se requiere a nivel nacional de la capacitación de jueces, fiscales, abogados y comerciantes, tanto de la pequeña como de la gran empresa, para promover el uso de Internet en un entorno seguro y fomentar el comercio electrónico.

## PARAGUAY

Mediante el Decreto N° 7706, del 15 de noviembre de 2011, la Presidencia de la República del Paraguay aprobó el Plan Director de Tecnologías de la Informa-

ción y Comunicación (TICs) del Poder Ejecutivo, que incluye entre las medidas para cerrar la brecha digital la estrategia para promover el comercio electrónico entre los distintos actores económicos. De conformidad con el Plan Director, el Congreso Nacional sancionó la Ley de Comercio Electrónico (Ley N° 4868/13), del 1 de marzo de 2013, principal cuerpo normativo que rige la materia en conjunción con la Ley de Validez Jurídica de la Firma Electrónica, la Firma Digital, los Mensajes de Datos y el Expediente Electrónico (Ley N° 4017/10), del 24 de diciembre de 2010 (Ley N° 4017/10), modificada mediante la Ley N° 4610, del 9 de mayo de 2012. Estas leyes incorporan diversas medidas de Leyes Modelo de la CNUDMI sobre Comercio Electrónico y las Firmas Electrónicas.

#### a) Transacciones electrónicas / Firmas electrónicas

Por lo que se refiere al ámbito nacional, la Ley de Comercio Electrónico (Ley N° 4.868/13) regula el comercio y la contratación realizados a través de medios electrónicos o tecnológicamente equivalentes entre Proveedores de Bienes y Servicios por vía electrónica (establecidos en Paraguay y fuera del país), intermediarios en la transmisión de contenido por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica y los consumidores o usuarios. También establece el régimen de exclusión de responsabilidad para los proveedores de servicios de intermediación, alojamiento de datos, enlaces y de copia temporal. Asimismo, establece los requisitos de información que deben cumplir los sitios web, además de conferir validez jurídica a los contratos celebrados por vía electrónica y a las facturas electrónicas. De igual forma, establece un catálogo de infracciones y sanciones.

Mediante Decreto N° 1165, del 27 de enero de 2014, la Presidencia del Paraguay aprobó el Reglamento de la Ley de Comercio Electrónico (Ley N° 4.868), del 26 de febrero de 2013, que otorga facultades al Ministerio de Industria y Comercio como Autoridad de Aplicación a través de la Dirección General de Firma Digital y Comercio Electrónico para interpretar y aplicar dicha Ley, en temas relacionados con: i) la contratación por vía electrónica a distancia con proveedores de bienes y servicios; ii) la organización y gestión de subasta por medios electrónicos o de mercados y centros comerciales virtuales; iii) la gestión de compras en la red por grupos de personas; iv) la distribución de contenidos a través de la red, previa petición individual que resulte en una actividad económica para el proveedor; v) el envío de comunicaciones comerciales; vi) los servicios de intermediación (acceso, transmisión de datos,

alojamiento, copia temporal, búsqueda), y vii) el suministro de información vía telemática.

Por su parte, la Ley N° 4017/10 reviste de especial relevancia toda vez que reconoce la validez jurídica de la firma electrónica, la firma digital, los mensajes de datos y el expediente electrónico y regula la utilización de los mismos, las empresas certificadoras, su habilitación y la prestación de los servicios de certificación. Distingue la firma electrónica de la firma digital, confiriéndoles diferentes efectos jurídicos y reconoce la equivalencia funcional de los documentos impresos respecto de los documentos consignados en mensajes de datos, así como de la firma manuscrita respecto de la firma digital, siempre y cuando esta última haya sido certificada por un prestador de servicios habilitado por el Ministerio de Industria y Comercio. También faculta a la Administración Pública para llevar a cabo trámites administrativos a través de medios electrónicos y a utilizar expedientes electrónicos y firmas digitales en sus actuaciones.

La Ley fue reglamentada por Decreto del Poder Ejecutivo N° 7369/2011 y amplió su alcance en virtud de la Ley N° 4610/12, del 9 de mayo de 2012, que la modificó parcialmente en cuanto al ámbito de aplicación de expedientes electrónicos y la designación del Ministerio de Industria y Comercio como Autoridad de Aplicación.

En el ámbito administrativo, la Ley de Contrataciones Públicas (Ley N° 2.051/03), aprobada el 12 de diciembre de 2002, modificada por la Ley N° 3439/07, aprobada el 31 de diciembre de 2007, establece el Sistema de Contrataciones del Sector Público, que tiene por objeto regular las acciones de planeación, programación, presupuesto, contratación, ejecución, erogación y control de las adquisiciones y locaciones de todo tipo de bienes, la contratación de servicios en general, los de consultoría y de las obras públicas y los servicios relacionados con las mismas además de regular la certificación de los medios de identificación electrónica para la contratación con el sector público.

En cuanto al uso de medios electrónicos en la gestión gubernamental, la Ley de Reordenamiento Administrativo y de Adecuación Fiscal (Ley N° 2421/04), aprobada el 25 de junio de 2005, obliga a la Subsecretaría de Estado de Tributación (SET) a contar con una página web regularmente actualizada, a fin de informar a los administrados sobre los servicios que ofrece y sus obligaciones fiscales. Actualmente, la Administración Tributaria permite que los contribuyentes utilicen servicios electrónicos para presentar declaraciones juradas o imprimir el formulario del Registro

Único del Contribuyente (RUC), entre otros. Cabe señalar que la Ley N° 2.422/04 - Código Aduanero, aprobada el 30 de junio de 2004, incorpora el uso de sistemas informáticos en las operaciones aduaneras para simplificar los procedimientos, permitiendo el uso de tecnologías de la información y la automatización de los procesos. De igual forma, establece que las firmas autógrafas que la Dirección Nacional de Aduanas requiera, pueden ser sustituidas por contraseñas o signos adecuados, así como por la firma electrónica para la sustanciación de las actuaciones administrativas que se realicen por medios informáticos. El Código reconoce que para todos los efectos legales, la clave de acceso confidencial y/o firma electrónica equivale a la firma autógrafa, y reglamenta el uso del expediente electrónico.

Asimismo, es preciso destacar que la República del Paraguay ha suscrito la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales (2005), sin embargo todavía no ha sido ratificada. También ha suscrito la Resolución del MERCOSUR N° 34/06, que aprueba las Directrices para la celebración de acuerdos de reconocimiento mutuo de firmas electrónicas avanzadas en el ámbito del MERCOSUR, resolución que no necesita ser incorporada al ordenamiento jurídico de los Estados partes para reglamentar aspectos de la organización o del funcionamiento del MERCOSUR; y la Resolución N° 37/06, de reconocimiento de la eficacia jurídica del documento electrónico, la firma electrónica y la firma electrónica avanzada en el ámbito del MERCOSUR; sin embargo, dicha resolución no ha sido todavía incorporada al derecho positivo paraguayo.

#### b) Protección al consumidor

Por lo que se refiere a la normativa relacionada con la protección al consumidor, la Ley de Defensa del Consumidor y Usuario (Ley N° 1334/98), del 30 de octubre de 1998, establece las normas para proteger su dignidad, salud, seguridad e intereses económicos. Los derechos reconocidos por esta Ley no son objeto de renuncia, transacción o limitación convencional por parte de los consumidores y deben prevalecer sobre cualquier norma legal, uso, costumbre, práctica o estipulación en contrario. Así, esta Ley regula todos los actos celebrados entre proveedores y consumidores relativos a la distribución, venta, compra o cualquier otra forma de transacción comercial de bienes y servicios. En el ámbito de las telecomunicaciones, la Ley N° 2340/03 amplía la Ley N° 1334/98, para adicionar un capítulo especial en materia de servicios de telecomunicaciones. Entre las principales medidas que

establece dicho capítulo se encuentra la obligación de proporcionar información que permita al consumidor identificar al proveedor, así como la obligación de proporcionar al consumidor información transparente sobre la facturación de los servicios.

Por su parte, la Ley de Comercio Electrónico (Ley N° 4868/13), del 26 de febrero de 2013, también establece a favor de los consumidores los siguientes derechos: i) oponerse a la utilización de sus datos con fines promocionales; ii) retractarse de la transacción comercial en el plazo de cinco días hábiles a partir de la recepción del producto o servicio, con la simple notificación electrónica de su voluntad; iii) obtener información completa y verdadera sobre los productos y servicios; iv) recibir el producto o servicio contratado en el tiempo, calidad y cantidad convenida, y v) reembolsar el dinero pagado en los casos de devoluciones. Por su parte, el Reglamento de la Ley de Comercio Electrónico obliga a los proveedores de bienes y servicios por vía electrónica a distancia a proporcionar a los consumidores o usuarios de forma transparente, clara y sencilla, la información con respecto a la seguridad de los medios de pago utilizados y la tecnología que se esté utilizando para proteger las transmisiones, procesamiento y/o almacenamiento de sus datos financieros.

En el ámbito internacional, es importante mencionar el Protocolo de Santa María, que ha sido ratificado por Paraguay mediante la Ley 1.081 de 07/97, que reconoce la jurisdicción del tribunal del Estado en que se encuentre el domicilio del consumidor. Asimismo, es preciso destacar la Resolución del MERCOSUR N° 21/04 - Derecho a la Información del Consumidor en las Transacciones Comerciales efectuadas a través de Internet y la Resolución del MERCOSUR N° 45/06 - Defensa del Consumidor - Publicidad Engañosa, las cuales han sido suscritas por Paraguay, pero que no han sido todavía internalizadas en su derecho positivo vigente.

#### c) Protección de datos personales

En cuanto al derecho a la vida privada y a la protección de datos personales, la Constitución Nacional del Paraguay, del 20 de junio de 1992, los ha reconocido como derechos fundamentales en concordancia con el Pacto de San José de Costa Rica, que consagra el derecho a la intimidad, personal y familiar, el respeto a la vida privada, a la dignidad del individuo y a su imagen privada. De igual manera, la constitución ha reconocido al Hábeas Data como un derecho fundamental que permite a toda persona acceder a la información y a los datos que sobre sí misma o sobre sus bienes obren en registros oficiales o privados de

carácter público, así como para conocer su uso y finalidad.

En virtud del Hábeas Data, el titular de los datos tiene la facultad de solicitar la actualización, la rectificación o la destrucción de aquellos datos que fuesen erróneos o afectasen ilegítimamente sus derechos. Adicionalmente, la Ley N° 1682/2001, que reglamenta la Información de Carácter Privado, aprobada el 28 de diciembre de 2000, modificada por la Ley N° 1969/02, del 6 de septiembre de 2002, establece normas que rigen el almacenamiento, la recolección, el procesamiento y la publicación de datos de carácter privado. Esta ley es de carácter general y no se limita a las bases de datos electrónicas. La Ley autoriza la publicación y difusión de datos que consistan en el nombre, apellido, documento de identidad, domicilio, edad, fecha y lugar de nacimiento, estado civil, ocupación o profesión, lugar de trabajo y teléfono ocupacional de las personas, que sean considerados datos personales públicos.

La Ley N° 4.868/13 establece que los proveedores no pueden vulnerar la protección de los datos personales y los derechos a la intimidad personal y familiar de las partes o los terceros intervinientes. También ordena que cuando los Proveedores de Bienes y Servicios empleen dispositivos de almacenamiento y recuperación de datos en equipos terminales, informarán a los consumidores o usuarios de manera clara y completa sobre su utilización y finalidad, ofreciéndoles la posibilidad de rechazar la utilización de los datos mediante un procedimiento sencillo y gratuito.

Asimismo, ordena que los proveedores de bienes y servicios por vía electrónica a distancia deben poner a conocimiento del consumidor o usuario la finalidad y el tratamiento que se le dará a sus datos personales conforme a la Ley vigente relativa a la materia. También lo debe comunicar al destinatario de los datos suministrados y al responsable de custodiar o almacenar la información proporcionada. El proveedor de bienes y servicios debe emplear sistemas seguros para evitar la pérdida, alteración y acceso de terceros no autorizados a los datos suministrados por el consumidor o usuario y debe recolectar el consentimiento expreso para tratar los datos personales de los consumidores.

#### d) Propiedad industrial e intelectual

En el ámbito de la propiedad intelectual, la Constitución Nacional garantiza a los autores, inventores, productores o comerciantes, la propiedad exclusiva de sus obras o invenciones, con arreglo a la Ley. Entre las principales leyes en la materia cabe mencionar la

Ley de Derecho de Autor y Derechos Conexos (Ley N° 1.328/98), del 27 de agosto de 1998, la Ley de Marcas (Ley N° 1.294/98), aprobada el 24 de junio de 1998, la Ley de Patentes de Invenciones (Ley N° 1.630/00), del 29 de noviembre de 2000, modificada por la Ley N° 2047/02, del 19 de diciembre de 2002, y la Ley N° 2593/05, del 17 de junio de 2005, la Ley de dibujos y modelos industriales (Ley N° 868/81), del 2 de noviembre de 1981, la Ley N° 1.582/00, que aprueba el Tratado de la OMPI sobre Derecho de Autor (WCT), aprobada el 6 de octubre de 2000, así como la Ley N° 1583, que aprueba el Tratado de la OMPI sobre Interpretación o Ejecución de Fonogramas (WPPT), aprobada el 6 de octubre de 2000. Adicionalmente, Paraguay también ha ratificado el Convenio de París y el Convenio de Berna.

#### e) Nombres de dominio

En cuanto a los nombres de dominio, el NIC-PY es la entidad encargada de administrar los nombres de dominio, y su operación se encuentra a cargo del Laboratorio de Electrónica Digital (LED) de la Universidad Católica Nuestra Señora de la Asunción y el Centro Nacional de Computación (CNC) de la Universidad Nacional de Asunción. No existen leyes que regulen la naturaleza jurídica del nombre de dominio, básicamente se rigen por el Reglamento Administrativo del organismo encargado. El NIC-PY actúa en calidad de coordinador del sistema de nombres de dominio y no tiene facultades jurisdiccionales, ni actúa como mediador ni como árbitro, y tampoco interviene en los conflictos que se susciten en torno a los nombres de dominio. Las controversias que se dirimen de manera extrajudicial se rigen por la Ley de Arbitraje y Mediación (Ley N° 1878/02).

#### f) Delitos Informáticos y Seguridad de la Información

Mediante la Ley N° 4439, del 3 de octubre de 2011, que modifica y amplía varios artículos de la Ley N° 1160/97 del Código Penal, se incorporaron los siguientes delitos informáticos: i) pornografía infantil; ii) acceso indebido a datos; iii) interceptación de datos; iv) preparación de acceso indebido e interceptación de datos; v) acceso indebido a sistemas informáticos; vi) sabotaje de sistemas informáticos; vii) estafa mediante sistemas informáticos, y viii) falsificación de tarjetas de débito o de crédito y otros medios electrónicos de pago.

En 2012 se conformó el CERT-PY, dependiente de la Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATICs), con el objetivo de facilitar y coordinar la protección de los sistemas cibernéticos y de la información que respaldan la infraestructura

nacional y gubernamental, y garantizar una respuesta eficaz y oportuna a los incidentes cibernéticos.

#### g) Iniciativas de Ley y retos

Entre los principales retos que enfrenta Paraguay se encuentra la disminución de las asimetrías respecto de los países de la región. En cuanto a la brecha digital, es preciso mejorar las condiciones de acceso a Internet y, de esa manera, lograr implementar una Internet más inclusiva y orientada al desarrollo. De igual forma, es necesario actualizar el marco legislativo procesal penal a fin de robustecer las capacidades del Estado para combatir los delitos informáticos. Asimismo, el marco normativo en materia de protección de datos requiere actualizarse a efectos de dar cumplimiento a los compromisos asumidos por Paraguay en la Red Iberoamericana de Protección de Datos.

## PERÚ

En el Plan de Desarrollo de la Sociedad de la Información en el Perú – La Agenda Digital 2.0, mediante Decreto Supremo N° 066-2011-PCM, de julio de 2001, se incluyó como estrategia el Desarrollo del Comercio Electrónico en su “Objetivo 5. Incrementar la productividad y competitividad a través de la innovación en la producción de bienes y servicios, con el desarrollo y aplicación de las TIC”. Adicionalmente, la Política Nacional de Gobierno Electrónico 2013-2017, aprobada mediante Decreto Supremo N° 081-2013, la Ley de Promoción de la Banda Ancha y Construcción de la Red Dorsal Nacional de Fibra Óptica (Ley N° 29904), del 20 de julio de 2012, y su Reglamento, del 4 de noviembre de 2013, así como el Decreto Legislativo N° 604 que aprueba la Ley de Organización y Funciones del Instituto Nacional de Estadística e Informática, del 30 de abril de 1990, constituyen medidas que robustecen el entorno para dar viabilidad al comercio electrónico.

Entre las principales leyes que rigen el comercio electrónico se encuentra la Ley N° 27291, del 24 de junio de 2000, que modifica al Código Civil, Ley de Firmas y Certificados Digitales, o Ley N° 27269, del 26 de mayo de 2000, modificada por la Ley N° 27310 - Ley de Firmas y Certificados Digitales, así como el Reglamento de la Ley de Firmas y Certificados Digitales (RLFCD) por Decreto Supremo N° 052-2008/PCM, aprobado el 18 de julio de 2008.

Por su parte, la Presidencia del Consejo de Ministros, a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), promueve en las instituciones públicas la adopción de las TIC para la prestación de sus servicios en línea y promueve el desarrollo

de seminarios en materia de “Gobierno Electrónico y Sociedad de la Información” para capacitar a los funcionarios públicos en temas relacionados con el gobierno electrónico y su marco jurídico, el gobierno abierto, las estadísticas TIC en el Estado, la Sociedad de la Información e Inclusión y Ciudadanía Digital para la Modernización del Estado y la mejora de la gestión pública.

#### a) Transacciones electrónicas / Firmas electrónicas

En materia de transacciones electrónicas, destaca la Ley N° 27291, que modifica al Código Civil, y señala que cuando la Ley establezca que la manifestación de voluntad deba hacerse a través de alguna formalidad expresa o requiera de firma, ésta podrá ser generada o comunicada por medios electrónicos, ópticos o cualquier otro análogo, y dispone que, en materia de contratación entre ausentes, la oferta, su revocación, su aceptación y cualquier otra declaración contractual se consideran conocidas en el momento en que llegan a la dirección del destinatario. Si se realizan a través de medios electrónicos, ópticos u otro análogo, se presumirá la recepción de la declaración contractual cuando el remitente reciba el acuse de recibo.

Por su parte, la Ley de Firmas y Certificados Digitales o Ley N° 27269 de 2000, reformada mediante la Ley N° 27310, que modifica el artículo 11 de la Ley N° 27269 de 2000, establece los lineamientos generales que rigen la firma digital y la certificación digital, así como las atribuciones de la autoridad competente y la actuación de las entidades de certificación y de registro o verificación. La Ley establece que la firma digital tiene la misma validez y eficacia jurídica que la firma manuscrita u otras análogas que conlleven una manifestación de voluntad. De igual forma, reconoce los certificados de firmas digitales emitidos por entidades extranjeras, siempre y cuando tales certificados sean reconocidos por la autoridad administrativa competente.

En este sentido, el Reglamento de la Ley de Firmas y Certificados Digitales (RLFCD) (Decreto Supremo N° 052-2008/PCM), promulgado por la Presidencia del Consejo de Ministros, y que refleja algunos temas previstos en la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas, fue emitido para regular en el ámbito del sector público como en el privado, la utilización de firmas electrónicas y el régimen de la Infraestructura Oficial de Firma Electrónica (IOFE). El Reglamento designa al Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOP) como Autoridad Administrativa Competente y al Registro Nacional de Identificación y Estado Civil (RENIEC) como Entidad de Certificación

Nacional para el Estado Peruano (ECERNEP), Entidad de Certificación para el Estado Peruano (ECEP) y Entidad de Registro o Verificación para el Estado Peruano (EREP).

El Reglamento otorga a la firma digital generada dentro de la Infraestructura Oficial de Firma Electrónica (IOFE) la misma validez y eficacia jurídica que a la firma manuscrita. De igual forma, señala que los documentos electrónicos firmados digitalmente en el marco de la IOFE deberán ser admitidos como prueba en los procesos judiciales y/o procedimientos administrativos. La IOFE es un sistema confiable, acreditado, regulado y supervisado por la Autoridad Administrativa Competente, provisto de instrumentos legales y técnicos que permiten generar firmas digitales y proporcionar diversos niveles de seguridad respecto de la integridad de los documentos electrónicos y de la identidad de su autor.

Mediante Decreto Supremo N° 070-2011-PCM, del 27 de julio de 2011, que modifica el Reglamento de la Ley N° 27269, Ley de Firmas y Certificados Digitales, y establece normas aplicables al procedimiento registral en virtud del Decreto Legislativo N° 681 y ampliatorias, se modifican los requerimientos en cuanto al contenido y la vigencia de los certificados digitales para las personas naturales y las personas jurídicas y se reconoce la atribución del INDECOPI para cumplir con su función de Autoridad Administrativa Competente de la IOFE.

De igual forma, en virtud del Decreto Supremo N° 105-2012-PCM, del 21 de octubre de 2012, se establecen disposiciones para facilitar la puesta en marcha de la firma digital y modifican el Decreto Supremo N° 052-2008-PCM, Reglamento de la Ley de Firmas y Certificados Digitales. Mediante el citado instrumento se permite a las personas naturales y jurídicas utilizar un certificado digital emitido por proveedores que cuenten con la certificación internacional Web Trust, hasta en tanto cuente con el certificado digital del INDECOPI.

Por su parte, la Comisión Nacional Supervisora de Empresas y Valores (CONASEV) emitió su Resolución N° 008 – 2003, del 7 de febrero de 2003, en virtud de la cual aprueba el Reglamento del Sistema MVNet, que regula el sistema de transmisión e intercambio de documentos e información a través de la Red del Mercado de Valores Peruano (MVNet), que opera con tecnología de PKI. Las personas naturales y jurídicas que se encuentren dentro del ámbito de supervisión y control de la Comisión deberán utilizar obligatoriamente esta Red, para remitirle toda la información y

documentación que se encuentran obligadas a proporcionar.

En el ámbito de las transacciones gubernamentales en línea, la Ley del Procedimiento Administrativo General (Ley N° 27444), del 10 de abril de 2001, regula, entre otros temas, las notificaciones vía medios electrónicos u otros medios que permitan comprobar fehacientemente su acuse de recibo y quién lo recibe, siempre que haya sido solicitado expresamente por el administrado. De igual forma autoriza el uso de medios electrónicos para las comunicaciones al interior de la Administración Pública.

Asimismo, autoriza a los administrados a solicitar el envío de información o documentación relacionada con un proceso administrativo a través de medios de transmisión a distancia.

En la actualidad, el Sistema Electrónico de Contrataciones del Estado ([www.seace.gob.pe](http://www.seace.gob.pe)) permite el intercambio de información y difusión sobre adquisiciones y contrataciones del Estado, así como la realización de transacciones electrónicas.

Por otra parte, con base en el Reglamento de la Ley de Firmas y Certificados Digitales (RLFCD) se faculta a la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) para supervisar los planes que las entidades de la Administración Pública elaboren con miras a la implementación de los procedimientos y trámites administrativos por medios electrónicos seguros.

En el ámbito fiscal, el Decreto Supremo N° 135-99, Código Tributario, del 19 de agosto de 1999, modificado por Decreto Legislativo N° 953, del 5 de febrero de 2004, faculta a la Administración Tributaria para autorizar la presentación de declaraciones a través de medios magnéticos, fax, transferencia electrónica o cualquier medio que cumpla las condiciones que establezca la Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT). Con base en ello, la SUNAT ha desarrollado los Programas de Declaración Telemática (PDT).

Asimismo, en virtud del Decreto N° 809, Ley General de Aduanas, del 19 de abril de 1996, y su Reglamento, aprobado mediante Decreto Supremo N° 011-2005-EF, del 26 de enero de 2005, que rigen las actividades aduaneras de las personas, mercancías y medios de transporte que crucen las fronteras aduaneras, se faculta a la Aduana para expedir normas y establecer procedimientos que regulen la emisión, transferencia, uso y control de la información, a través de medios documentales, magnéticos o electrónicos,

a efectos de promover el desarrollo y facilitación de las actividades aduaneras. En este sentido, el Ministerio de Comercio Exterior y Turismo (MINCETUR) tiene a su cargo el desarrollo del sistema de Ventanilla Única de Comercio Exterior (VUCE), creada mediante Decreto Supremo N° 165-2006-MEF, del 3 de noviembre de 2006, otorgándose rango de Ley a su creación a través de la Primera Disposición Complementaria del Decreto Legislativo N° 1036, del 24 de junio de 2008.

La VUCE permite a las partes involucradas en el comercio y transporte internacional gestionar, a través de medios electrónicos, los trámites requeridos por las diversas entidades competentes, de acuerdo con la normatividad vigente, o solicitados por dichas partes para el tránsito, ingreso o salida del territorio nacional de las mercancías, y la instrumentación de las disposiciones en materia de comercio electrónico consignadas en los Tratados de Libre Comercio con Estados Unidos de Norteamérica y Canadá, así como los compromisos del Grupo de Comercio Electrónico del APEC en materia de comercio sin papel.

#### b) Protección al consumidor

La Ley N° 29571, Código de Protección y Defensa del Consumidor, del 1 de septiembre de 2010, contiene diversas medidas para proteger a los consumidores en línea. Entre las medidas más relevantes se encuentra la facultad que se otorga al consumidor para desvincularse del contrato utilizando los mismos mecanismos de forma, lugar y medios utilizados para la celebración de los contratos, incluyendo los medios electrónicos. También establece que los proveedores deben acreditar que entregaron oportunamente a los usuarios en línea copia de los contratos, incluyendo las condiciones generales de contratación, y deben proporcionar información sobre su identificación, domicilio, correo electrónico y otros datos de contacto.

Asimismo, prohíbe realizar proposiciones no solicitadas por correo electrónico, de manera persistente o ignorando la petición del consumidor para que cese este tipo de actividades. También prohíbe el envío de mensajes electrónicos masivos para promover productos y servicios, así como prestar el servicio de telemarketing a las direcciones electrónicas que hayan sido incorporadas en el registro implementado por el Indecopi para registrar a los consumidores que no deseen recibir este tipo de promociones. También dispone que los establecimientos comerciales deben contar con un Libro de Reclamaciones, en forma física o virtual.

Mediante Decreto Supremo N° 011-2011-PCM, aprobado el 28 de febrero de 2011, se aprobó el Re-

glamento del Libro de Reclamaciones del Código de Protección y Defensa del Consumidor, siendo este modificado mediante Decreto Supremo N° 006-2014-PCM, del 23 de enero de 2014, que señala respecto al Libro de Reclamaciones, que cada establecimiento comercial abierto al público deberá contar con un Libro de Reclamaciones, donde los proveedores que utilicen medios virtuales para establecer sus relaciones de consumo deberán implementar un Libro de Reclamaciones Virtual en cada uno de sus establecimientos y deberán brindar el apoyo necesario para que el consumidor ingrese su queja o reclamo en el Libro de Reclamaciones.

La Ley de Represión de la Competencia Desleal, adoptada mediante Decreto Legislativo N° 1044, del 25 de junio de 2008, regula la publicidad en línea y faculta al INDECOPI para sancionar a quienes utilizando medios electrónicos, incluyendo el Internet, difundan información que impida el adecuado funcionamiento del proceso competitivo, mediante actos que induzcan a los consumidores al engaño o la confusión.

#### c) Protección de datos personales

La Ley de Protección de Datos Personales (Ley N° 29733), del 3 de julio de 2011, está en consonancia con las Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana emitidas por la Red Iberoamericana de Protección de Datos Personales. La Ley protege los datos personales, automatizados o no, de toda persona natural o jurídica, y el manejo de esta información en bancos de datos públicos o privados, a efectos de garantizar el derecho a la privacidad de las personas. La Autoridad Nacional de Protección de Datos Personales, adscrita a la Dirección Nacional de Justicia del Ministerio de Justicia y Derechos Humanos, es la entidad a cargo de supervisar la aplicación de la Ley. La Ley distingue los datos personales de los datos sensibles. También establece la obligación de registrar los bancos de datos públicos o privados en el Registro Nacional de Protección de Datos Personales y prohíbe la transferencia de datos personales a países que no proporcionen niveles de seguridad y protección adecuados.

Las personas naturales, las personas jurídicas de derecho privado y las entidades públicas que hacen uso, almacenan o transfieren información privada de los titulares de los datos se encuentran obligadas a: i) que el uso de la información sea adecuado, proporcional y necesario en relación con el ámbito y las finalidades para el que se colecta; ii) obtener consentimiento del titular para la entrega de los datos; iii) usar los datos para los fines que motivaron su obtención, y iv) adoptar las medidas técnicas, organizativas y legales para

garantizar la seguridad y confidencialidad de los datos personales.

La violación a la Ley se castiga con sanciones administrativas y penales. La Ley otorga al titular de los datos el derecho a la información, el derecho de acceso, derecho de actualización, inclusión, rectificación y supresión, así como el derecho de oposición, derecho a impedir el suministro, derecho al tratamiento objetivo y el derecho a la indemnización. La Ley clasifica las infracciones en leves, graves y muy graves, estableciendo sanciones administrativas, con independencia de la responsabilidad civil y penal que pueda derivar.

Mediante el Reglamento de la Ley de Protección de Datos Personales (Ley N° 29733), emitido mediante Decreto Supremo N° 003-2013-JUS, del 22 de marzo de 2013, y con la Directiva de Seguridad de la Información Administrada por los Bancos de Datos Personales, emitida por la Autoridad Nacional de Datos Personales, de octubre de 2013, se completa el régimen normativo para la protección de los datos personales.

#### d) Propiedad industrial e intelectual

En materia de propiedad intelectual, en virtud del Decreto Legislativo N° 822, Ley sobre el Derecho de Autor, del 23 de abril de 1996, la normativa del Perú incorpora diversas medidas contenidas en el Convenio de Berna, el ADPIC, la Decisión 351 de la Comisión del Acuerdo de Cartagena, que aprueba el Régimen Común sobre Derechos de Autor y Derechos Conexos. La Ley protege a los autores de las obras literarias y artísticas, así como a sus derechohabientes y a los titulares de los derechos conexos al derecho de autor. Asimismo, regula las sociedades de gestión colectiva y protege a los autores de las bases de datos, en términos similares a los establecidos en el ADPIC. En virtud del Decreto Legislativo N° 1076, la Ley Modificatoria del Decreto Legislativo N° 822, del 27 de junio de 2008, incorpora la utilización de medidas tecnológicas para la protección de obras y los sistemas de información sobre la gestión de derechos.

Es importante señalar que, en el ámbito internacional, Perú ha suscrito:

- los Tratados de Internet de la OMPI, tanto el WCT como el WPPT, y
- el Tratado de Beijing sobre Interpretaciones y Ejecuciones Audiovisuales.

En el ámbito de la propiedad industrial, el Decreto Legislativo N° 823, Ley de Propiedad Industrial, del 23 de abril de 1996, incorporó distintas medidas de la Decisión 344 de la Comisión del Acuerdo de Carta-

gena, el Régimen Común sobre Propiedad Industrial para los Países Andinos, el Convenio de París para la Protección de la Propiedad Industrial y el ADPIC. La Ley regula, entre otras cuestiones, las patentes de invención, los certificados de protección, los modelos de utilidad, los diseños industriales, los secretos industriales, las marcas, los nombres comerciales, los lemas comerciales y las denominaciones de origen. Entre las medidas importantes para combatir la piratería, Perú adoptó el Decreto Legislativo N° 1092, del 27 de junio de 2008, que aprueba medidas en frontera para la protección de los derechos de autor y derechos conexos y los derechos de marcas.

#### e) Nombres de dominio

En materia de nombres de dominio, la Red Científica Peruana se encarga de administrar los dominios peruanos (.pe) y ha adoptado dentro de sus políticas de resolución de disputas los principios de la Política uniforme de solución de controversias en materia de nombres de dominio de la ICANN, y reconoce como instancias para resolver las controversias al Centro de Arbitraje y Mediación de la OMPI y al Cibertribunal Peruano.

#### f) Delitos Informáticos y Seguridad de la Información

En el ámbito penal, con la Ley N° 30171, del 10 de marzo de 2014, que modifica la Ley de Delitos Informáticos (Ley N° 30096), se amplió el contenido de diversos tipos penales, incluyendo los delitos de: i) acceso ilícito a sistemas informáticos; ii) atentado a la integridad de datos informáticos; iii) atentado a la integridad de sistemas informáticos; iv) pornografía infantil por medios tecnológicos; v) interceptación de datos informáticos; vi) fraude informático; vii) abuso de mecanismos y dispositivos informáticos, y viii) tráfico ilegal.

De igual forma, se establecieron medidas de coordinación interinstitucional entre la Policía Nacional, el Ministerio Público y otros organismos especializados. También se establecieron disposiciones para exentar de responsabilidad penal a los prestadores de servicios de telecomunicaciones. Asimismo, se incluyeron medidas para llevar a cabo la intervención, grabación o registro de comunicaciones telefónicas o de otras formas de comunicación y geolocalización de teléfonos móviles.

En materia de seguridad de la información, desde 2009 se constituyó el PeCERT, equipo de respuesta a incidentes de seguridad cibernéticos (CSIRT) peruano, que ha desempeñado un papel relevante en la atención a los incidentes informáticos.

### g) Iniciativas de Ley y retos

Entre los principales retos que enfrenta Perú se encuentra su adhesión al Convenio del Consejo de Europa sobre la Ciberdelincuencia, a efectos de robustecer la cooperación internacional para la investigación y persecución de los delitos informáticos. De igual forma, hace falta constituir una agencia que coordine de manera armónica las políticas y la regulación sobre la sociedad de la información, que marque un rumbo conjunto hacia la autoridad de transparencia y acceso a la información, la comisión de datos espaciales, el Pe-CERT, la autoridad de datos personales, el sistema de firma digital, las políticas de alfabetización digital y los instrumentos de gobierno electrónico y de comercio electrónico.

## REPÚBLICA DOMINICANA

La República Dominicana ha sentado las bases normativas para promover el comercio electrónico como una herramienta para el desarrollo nacional y, en virtud de la Ley de Estrategia Nacional de Desarrollo 2030 (Ley No. 1-12), del 25 de enero de 2012, la República Dominicana plantea el uso de las TIC como instrumento para incrementar la productividad de las empresas, mejorar la gestión pública mediante servicios públicos más eficientes y accesibles. Adicionalmente, la Ley sobre el Comercio Electrónico, Documentos y Firmas Digitales (Ley No. 126-02), del 4 de septiembre de 2002, incorpora diversos preceptos de la Ley Modelo de la CNUDMI sobre Comercio Electrónico.

### a) Transacciones electrónicas / Firmas electrónicas

La Ley sobre el Comercio Electrónico, Documentos y Firmas Digitales (Ley No. 126-02) es el principal ordenamiento en materia de transacciones electrónicas y de firmas electrónicas. Define “comercio electrónico” como toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más documentos digitales o mensajes de datos o de cualquier otro medio similar. La Ley promueve la facilitación del comercio y reconoce la validez de las transacciones a través de medios electrónicos, así como la equivalencia funcional entre los documentos digitales y los mensajes de datos respecto de los documentos impresos, y de la firma digital respecto de la firma manuscrita. También reconoce su valor probatorio.

Asimismo, regula las entidades de certificación encargadas de emitir certificados digitales relacionados con las firmas digitales, así como de ofrecer o facilitar los servicios de registro y estampado cronológico

de la transmisión y recepción de mensajes de datos. Respecto de la formación de los contratos, la Ley establece que la oferta y su aceptación pueden expresarse por medio de documentos digitales o de mensajes de datos. También reconoce los certificados digitales emitidos por entidades de certificación extranjeras.

En materia financiera, la Ley faculta a la Junta Monetaria para normar todo lo atinente a las operaciones y servicios financieros asociados a los medios de pago electrónicos que realice el Sistema Monetario y Financiero de la República Dominicana. En este sentido, la Junta Monetaria emitió el Reglamento de Sistemas de Pago que establece el régimen jurídico aplicable al sistema de pago y liquidación de valores de la República Dominicana (SIPARD).

Mediante la Ley Monetaria y Financiera (Ley No. 183-02), del 21 de noviembre de 2002, se faculta a la Junta Monetaria para determinar los requisitos que deben observarse para la admisión de pruebas por medios electrónicos en materia bancaria y para las operaciones con tarjeta de débito y crédito, así como con cualquier otro instrumento de pago, cualesquiera que sea su base material o electrónica.

En el ámbito gubernamental, la Ley No. 126-02 determina que cuando cualquier norma exija la presencia de una firma o establezca ciertas consecuencias en ausencia de la misma, se entenderá satisfecho dicho requerimiento en relación con un documento digital o un mensaje de datos, si este ha sido firmado digitalmente y la firma digital cumple con los requisitos de validez establecidos en esa Ley. Asimismo, establece que en toda interacción con una entidad pública que requiera de un documento firmado, este requisito se podrá satisfacer con uno o más documentos digitales o mensajes de datos que sean firmados digitalmente conforme a los requerimientos contenidos en esa Ley.

Mediante Decreto No. 335-03 que aprueba el Reglamento de Aplicación de la Ley No. 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales, del 8 de abril de 2003, se establecen con mayor detalle las facultades del Instituto Dominicano de las Telecomunicaciones (INDOTEL) y se determinan los requisitos que deben cumplir las entidades certificadoras. Asimismo, en virtud de la Resolución No.10-04, del 30 de enero de 2014 (norma complementaria) de la Ley No.126-02, el INDOTEL aprobó las Normas Complementarias, entre ellas, la Norma sobre Procedimientos de Autorización y Acreditación, que prescribe los aspectos generales, los requisitos y

el procedimiento para solicitar al INDOTEL la debida autorización para operar como Unidad de Registro.

En materia fiscal, la Ley de Rectificación Tributaria (Ley No. 495-06), del 28 de diciembre de 2006, incorpora la facultad de almacenar la información vinculada con la materia imponible en medios de almacenamiento de datos utilizados en sistemas de computación. De igual forma, faculta a los contribuyentes para conservar su contabilidad, incluyendo recibos o comprobantes de pago en medios electrónicos por 10 años. También autoriza a los contribuyentes a registrar ante las autoridades fiscales los códigos de identificación y acceso (PIN) para realizar declaraciones juradas, consultas, liquidación y pagos de tributos, así como otras gestiones a través de medios electrónicos, y se otorga la misma fuerza probatoria que a los actos bajo firma privada.

En el ámbito del comercio exterior, la Ley para el Régimen de las Aduanas (Ley No. 3489) no hace referencia a los medios electrónicos para las operaciones vinculadas con el despacho aduanero, sin embargo, en virtud del Decreto No. 248-09, del 9 de julio del 1998, se creó el Sistema Integrado de Ventanilla Única de Comercio Exterior (SIVUCEX), el cual instrumenta un sistema de procedimientos automatizados para el manejo de todos los trámites y servicios necesarios para el proceso de exportación por vía electrónica.

En el ámbito internacional, es preciso señalar la Resolución No.6-12, del 2 de febrero de 2012, que aprueba la adhesión a la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales.

#### b) Protección al consumidor

La Ley General de Protección de los Derechos del Consumidor o Usuario (Ley No. 358-05), del 6 de septiembre de 2005, desarrolla los derechos básicos de los consumidores de conformidad con lo previsto en la Resolución 39/248 sobre las Directrices de las Naciones Unidas para la Protección al Consumidor, del 9 de abril de 1985. En materia de comercio electrónico, la Ley obliga al proveedor a: i) informar previamente al consumidor sobre el precio, incluyendo los impuestos, forma y fecha de entrega, costo de envío y, en su caso, sobre el seguro correspondiente; ii) emitir una nota de remisión con el nombre y la dirección del proveedor y la consignación precisa del bien o servicio a nombre del consumidor; iii) tener constancia de que la entrega del producto o la prestación del servicio se haga al consumidor; iv) permitir al consumidor hacer reclamaciones, devoluciones o cambios por medios similares a los utilizados para la venta; v) cubrir los

costos de envío en caso de reposición o reparaciones cubiertas por la garantía; vi) prever y permitir al consumidor un plazo de reflexión, de tres (3) días hábiles como mínimo, previo a la entrega del bien o prestación del servicio; vii) prever y permitir al consumidor un plazo de prueba, de siete (7) días hábiles como mínimo, previo a la devolución del bien o la suspensión del contrato de prestación del servicio, y viii) emitir y entregar al consumidor o usuario una factura en formato escrito o digital.

#### c) Protección de datos personales

El derecho a la protección de datos personales está tutelado en la Constitución de la República Dominicana del 26 de enero de 2010. De conformidad con el texto constitucional y con los compromisos contraídos con la Red Iberoamericana de Protección de Datos, la Ley Orgánica sobre Protección de Datos de Carácter Personal (Ley No. 172-13), del 13 de diciembre de 2013, tutela la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos o privados, así como a garantizar que no se lesione el derecho al honor y a la intimidad de las personas. La Ley incorpora también diversas medidas que rigen a las Sociedades de Información Crediticia (SIC), así como la prestación de los servicios de referencias crediticias y el suministro de la información en el mercado, garantizando el respeto a la privacidad y los derechos de los titulares de la información.

La Ley reconoce los principios de información, consentimiento, calidad, licitud, lealtad, confidencialidad, seguridad y finalidad que deben regir en el tratamiento de los datos. Establece el deber de garantizar a los titulares de las informaciones el ejercicio pleno y efectivo del derecho de Hábeas Data o de la información, el cual se hace valer ante la autoridad judicial. Asimismo, obliga a conservar la información bajo las debidas condiciones de seguridad. También tutela el derecho de las personas al acceso, la actualización, la oposición al tratamiento, la rectificación o destrucción de los datos que les afecte ilegítimamente.

Por otra parte, la Ley No. 310-14, que regula el envío de correos electrónicos comerciales no solicitados (SPAM), del 11 de junio de 2014, regula el envío de comunicaciones comerciales, publicitarias o promocionales no solicitadas, realizadas vía correo electrónico, sin perjuicio de las disposiciones vigentes en materia comercial sobre publicidad y protección al consumidor. La Ley ordena que toda comunicación comercial electrónica debe contener el señalamiento "publicidad" en el campo del asunto de cada mensaje.

También señala que en caso de contenido sexual en la comunicación, que solo deba ser leído por mayores de edad, se incluirá la frase “publicidad para adultos”.

La Ley plantea que la comunicación comercial electrónica remitida desde una dirección de correo electrónico debe permitir al receptor comunicar su voluntad de no recibir comunicaciones comerciales. También señala que la comunicación debe incluir el nombre o razón social, domicilio completo y dirección de correo electrónico del iniciador de la comunicación. De igual forma, obliga a incluir un número de teléfono válido y activo, o de una dirección de correo electrónico válida y activa de respuesta, para que el destinatario pueda enviar un mensaje para notificar su voluntad de no recibir más comunicaciones comerciales.

La Ley prohíbe la remisión directa o indirecta de comunicaciones comerciales cuya recepción no haya sido solicitada o consentida por el interesado receptor. No obstante, señala que el envío de comunicaciones comerciales no solicitadas, no dará lugar a las acciones y sanciones previstas, cuando el destinatario tenga o haya tenido relación comercial previa con el iniciador de la comunicación o cuando el destinatario hubiese manifestado su consentimiento para recibir la comunicación. También prohíbe las comunicaciones cuando se remitan directa o indirectamente sin haber sido solicitadas o consentidas expresamente por el interesado receptor, o cuando el contenido de la información sea falso o engañoso en el campo del asunto, o que no coincida con el contenido del mensaje.

En el ámbito internacional, el Acuerdo de Asociación Económica entre los países miembros del Foro del Caribe del Grupo de Estados de África, el Caribe y el Pacífico (CARIFORUM) y la Comunidad Europea establece la obligación de los países miembros de garantizar el derecho a la intimidad con respecto al tratamiento de datos personales.

#### d) Propiedad industrial e intelectual

La Constitución reconoce como derechos de la persona humana la propiedad exclusiva por el tiempo y la forma que determine la ley, de los inventos y descubrimientos, así como de las producciones científicas, artísticas y literarias.

Por su parte, la Ley sobre Propiedad Industrial (Ley No. 20-00), del 4 de abril de 2000, establece que no considera como invenciones susceptibles de patente a los métodos matemáticos ni a los programas de ordenador. Por lo que se refiere al uso de las marcas, la Ley No. 20-00 no hace referencia al uso de las mismas en Internet o en direcciones de nombres de dominio.

En materia de derecho de autor, la Ley No. 65-00 sobre Derecho de Autor, del 26 de julio de 2000, considera a los programas de ordenador y a las bases de datos dentro de las obras protegibles. En cuanto a los derechos conexos de artistas, intérpretes, ejecutantes y organismos de radiodifusión, define los conceptos de fonogramas y videogramas y reconoce el derecho de comunicación pública por cualquier medio.

Por lo que se refiere al ámbito internacional de los derechos de propiedad intelectual, es preciso señalar que la República Dominicana ha ratificado

- los Tratados de la OMPI sobre Derecho de Autor (WCT) y sobre Interpretación o Ejecución y Fonogramas (WPPT);
- el Protocolo al Convenio Centroamericano para la Protección de la Propiedad Industrial;
- el Tratado de Libre Comercio entre la República Dominicana, Centroamérica y Estados Unidos (CAFTA-RD);
- el Convenio de París para la Protección de la Propiedad Industrial (1883);
- el Convenio de Berna para la Protección de las Obras Literarias y Artísticas;
- el Convenio de Ginebra para la protección de los productores de fonogramas contra la reproducción no autorizada de sus fonogramas;
- la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma), y
- el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (ADPIC), administrado por la Organización Mundial del Comercio (OMC).

#### e) Nombres de dominio

En materia de nombres de dominio, el NIC de la República Dominicana (<http://www.nic.do>), centro adscrito a la Pontificia Universidad Católica Madre y Maestra, es la entidad que administra los nombres de dominio de nivel superior de código de país “.do”. Entre las políticas del NIC de la República Dominicana no se hace referencia a la Política uniforme de solución de controversias en materia de nombres de dominio de la ICANN; sin embargo, se establece que el solicitante del registro del nombre de dominio debe asegurarse de que no está violando ninguna marca registrada. En caso de disputa entre solicitantes por los derechos de un nombre en particular, la autoridad que registra el nombre no adquiere responsabilidad alguna al registrarlo, solamente proveerá de información a ambas

partes. Sin embargo, dicha autoridad se reserva el derecho de revocar la delegación de un dominio a una organización o individuo, en caso de que la organización que posee el registro de marca de este dominio solicite su delegación.

#### f) Delitos informáticos y Seguridad de la información

La Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología, del 23 de abril de 2007, adopta diversas disposiciones previstas en el Convenio del Consejo de Europa sobre la Ciberdelincuencia, tanto a nivel sustantivo al tipificar delitos vinculados con los sistemas informáticos como a nivel procesal mediante la adopción de mecanismos que favorecen el combate efectivo a esta modalidad de delitos, facilitando la cooperación entre el Estado y el sector privado para la detección, investigación y sanción a nivel nacional de este tipo de delitos, y estableciendo disposiciones que permiten una cooperación internacional fiable y rápida.

La Ley define los Delitos de Alta Tecnología como aquellas conductas atentatorias a los bienes jurídicos protegidos por la Constitución, las leyes, los decretos, los reglamentos y las resoluciones relacionadas con los sistemas de información. Establece diversas definiciones, en las cuales destacan las referentes al acceso ilícito, la clonación, los códigos maliciosos, los datos relativos a los usuarios, el desvío de facilidades contratadas, la interceptación y la transferencia electrónica de fondos.

La Ley tipifica diversos delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas de información, así como delitos de contenido, delitos de propiedad intelectual, delitos contra las telecomunicaciones, y delitos contra la Nación y Actos de Terrorismo.

También determina los organismos competentes para investigar y perseguir los delitos informáticos, destacándose la interacción del Ministerio Público con el Departamento de Telecomunicaciones, Propiedad Intelectual y Comercio Electrónico de la Procuraduría General de la República. Se crea la Comisión Interinstitucional contra Crímenes y Delitos de Alta Tecnología (CICDAT) y el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT), siendo esta última el punto de contacto oficial de la República Dominicana en la Red Internacional 24/7 de Asistencia en Crímenes que Involucran Alta Tecnología perteneciente al Subgrupo de Crímenes de Alta Tecnología del Grupo de Expertos en Crimen Organizado Transnacional G8.

Asimismo, regula distintas medidas cautelares y procesales, incluyendo las reglas aplicables para la obtención y preservación de los datos contenidos en un sistema de información o sus componentes, datos de tráfico, conexión, acceso o cualquier otra información de utilidad, en la investigación de los delitos penalizados en la ley.

De igual forma, obliga a los proveedores de servicio a conservar los datos de tráfico, conexión, acceso o cualquier otra información que pueda ser de utilidad a la investigación, por un período mínimo de noventa (90) días.

Por su parte, la Ley N° 310-14, que regula el envío de correos electrónicos comerciales no solicitados (SPAM), del 8 de agosto de 2014, tipifica como delitos informáticos las siguientes conductas: i) acceder a un sistema informático sin autorización e intencionalmente iniciar la transmisión de comunicaciones comerciales desde o a través de dicho sistema; ii) acceder a un sistema informático para reenviar o retransmitir comunicaciones comerciales con la intención de engañar a los destinatarios sobre el origen de las mismas; iii) falsificar el campo del asunto de un mensaje de datos que contenga una comunicación comercial e intencionalmente iniciar la transmisión del mismo; iv) registrar y recolectar, fraudulenta o maliciosamente, usando información falsa, la identidad del registrante de una cuenta de correo electrónico o direcciones de correo electrónico de sitios de acceso público, tales como sitios de charla, directorios públicos, grupos receptores de noticias, servicios de perfiles en línea, redes sociales y cualquier otro medio masivo que agrupe direcciones electrónicas, o de un nombre de dominio e iniciar intencionalmente la transmisión de múltiples comunicaciones comerciales desde cualquier combinación de tales cuentas o dominios sin la autorización del titular del correo electrónico o del operador del sitio de acceso, y v) ofrecer la venta de bases de datos con direcciones de correos electrónicos sin el consentimiento expreso de los propietarios de los mismos, con el objetivo de generar comunicaciones comerciales no solicitadas.

#### g) Iniciativas de Ley y retos

Entre los retos que enfrenta la República Dominicana se encuentra la necesidad de contar con una estrategia o política nacional sobre seguridad cibernética a gran escala, así como con un CERT nacional para la atención de incidentes en materia de ciberseguridad.

## URUGUAY

La Agenda Digital de Uruguay 2011-2015 plantea, en el marco de sus objetivos, el desarrollo del comercio electrónico y de iniciativas que promuevan la inclusión financiera de los ciudadanos de ese país. Entre los principales instrumentos normativos que rigen las operaciones de comercio electrónico se encuentra la Ley de Admisibilidad, validez y eficacia jurídicas del documento electrónico y de la firma electrónica (Ley N° 18.600), del 21 de septiembre de 2009, al igual que la Ley de Defensa del Consumidor (Ley N° 17.250), del 17 de agosto de 2000, la Ley N° 18.331 de Protección de Datos Personales y Acción de “Hábeas Data”, del 11 de agosto de 2008, y la Ley de Inclusión Financiera (Ley N° 19.210), del 9 de mayo de 2014, cuyos contenidos se analizan en los siguientes apartados.

### a) Transacciones electrónicas / Firmas electrónicas

En materia de transacciones electrónicas se ha promulgado la Ley 16.879, del 3 de noviembre de 1997, que aprueba la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías, la cual menciona dentro de los medios para manifestar el consentimiento sobre diversos actos vinculados con el contrato de compraventa al teléfono, el télex u otros medios de comunicación instantánea. Adicionalmente, en virtud del Decreto N° 174/005, del 6 de junio de 2005, se incorpora al ordenamiento jurídico interno la Resolución No. 17/04 del Grupo Mercado Común del MERCOSUR, que aprueba la norma relativa a la informatización del manifiesto internacional de cargas/declaración de tránsito aduanero.

Adicionalmente, la Ley de Admisibilidad, validez y eficacia jurídicas del documento electrónico y de la firma electrónica (Ley N° 18.600), del 21 de septiembre de 2009, distingue la firma electrónica de la firma electrónica avanzada, confiriéndoles diferentes efectos jurídicos, y reconoce la equivalencia funcional de los documentos impresos respecto de los documentos consignados en mensajes de datos, así como de la firma manuscrita respecto de la firma digital, que ha sido certificada por un prestador de servicios acreditado. También faculta a las autoridades del Estado de los distintos poderes para llevar a cabo trámites administrativos a través de medios electrónicos y a utilizar expedientes electrónicos y firmas digitales en sus actuaciones, sea entre sí o con los particulares.

La Ley regula los servicios de certificación electrónica, designa a la Agencia de Gobierno Electrónico y Sociedad de la Información (AGESIC) como Autoridad

Certificadora Raíz Nacional y confiere a la Unidad de Certificación Electrónica –órgano desconcentrado de la AGESIC– facultades de: i) acreditación de los prestadores de servicios de certificación; ii) control sobre la calidad y confiabilidad de los servicios de certificación acreditados; iii) instrucción para recibir y evaluar reclamos de los titulares de certificados; iv) regulación, y v) sanción para los prestadores de servicios que incumplan la ley.

Por su parte, el Decreto de fecha 8 de diciembre de 2011 reglamenta la Ley relativa al documento electrónico y firma electrónica (Ley N° 18.600), que regula la Infraestructura Nacional de Certificación Electrónica y establece el sistema jerárquico, encabezado por la Agencia de Gobierno Electrónico y Sociedad de la Información (AGESIC) como Autoridad Certificadora Raíz Nacional, como la primera autoridad de la cadena de certificación a la cual le compete emitir, distribuir, revocar y administrar los certificados de los prestadores de servicios de certificación acreditados.

Asimismo, destaca la Ley de Rendición de Cuentas y Balance de Ejecución Presupuestal del Ejercicio 2006 (Ley N° 18.172), del 7 de septiembre de 2007, que crea el Registro de Prestadores de Servicios de Certificación a cargo de la Unidad Reguladora de Servicios de Comunicaciones (URSEC), la cual se encarga, entre otras cuestiones, de controlar la calidad y confiabilidad de los servicios brindados por los Prestadores de Servicios de Certificación

De igual forma, es preciso mencionar la Ley de Servicios Públicos y Privados, Seguridad Pública y Condiciones en las que se Desarrollan las Actividades Productivas (Ley N° 17.243), del 6 de julio de 2000, que regula la utilización de la firma electrónica, la firma digital, los servicios de certificación y el expediente electrónico en el ámbito administrativo. La Ley reconoce el empleo de la firma digital y su eficacia jurídica para otorgar seguridad a las transacciones electrónicas, permitiendo la identificación de las partes que participan en la misma. Por su parte, la Ley de Expediente Electrónico (Ley N° 18.237), del 9 de enero de 2008, autoriza el uso de expedientes electrónicos, documentos electrónicos, claves informáticas simples, firmas electrónicas, firmas digitales, comunicaciones electrónicas y domicilios electrónicos constituidos, en todos los procesos judiciales y administrativos que se tramitan ante el Poder Judicial.

Por su parte, la Ley de Inclusión Financiera (Ley N° 19.210), del 9 de mayo de 2014, autoriza a que el pago de salarios, jubilaciones y honorarios profesionales se realice a través de depósitos en cuentas bancarias

o en instrumentos de dinero electrónico. Asimismo, regula el dinero electrónico en el sistema financiero uruguayo y regula las cuentas bancarias con institutos de intermediación financiera. Plantea un cronograma de incorporación de 2 años para su implementación e impone restricciones al uso de dinero en efectivo. También establece incentivos tributarios para el uso de tarjetas, tanto de débito como de crédito, reduciendo la tasa del Impuesto al Valor Agregado (IVA).

En materia de impuestos y aduanas, se han emitido diversas normas, entre las cuales destaca la Ley del Sistema Tributario (Ley N° 18.083), del 18 de enero de 2007, que exenta del Impuesto a las Rentas de las Actividades Económicas (IRAE) y del Impuesto a las Rentas de las Personas Físicas (IRPF) a las rentas generadas por la producción de soportes lógicos y otros desarrollos en biotecnología y bioinformática. De igual forma, el Decreto N° 208/007, del 18 de junio de 2007, reglamenta las exoneraciones del Impuesto a las Rentas de las Personas Físicas (IRPF) en materia de nuevas tecnologías. Mientras que el Decreto N° 150/007, del 26 de abril de 2007, reitera la declaración de Interés Nacional de la actividad de producción del sector software, en condiciones de competencia internacional y exonera del Impuesto a las Rentas de las Actividades Económicas (IRAE) a las rentas derivadas de la actividad de producción de soportes lógicos hasta el 31 de diciembre de 2009.

De igual forma, es preciso mencionar el Decreto 341/003, del 26 de agosto de 2003, que establece el sistema de prestación de declaraciones juradas de determinados contribuyentes por Internet, así como el Decreto N° 148/002, del 30 de abril de 2002, que reglamenta los pronósticos de resultados deportivos internacionales y juegos de azar realizados vía Internet, y el Decreto N° 506/001, del 4 de enero de 2002, que establece un nuevo régimen de encomiendas postales internacionales como consecuencia de las que responden a operaciones de comercio electrónico.

Además, se han emitido diversos decretos que establecen exoneraciones sobre el Impuesto a las Rentas de la Industria y Comercio (IRIC) y el IVA en materia de nuevas tecnologías, sobre todo para los soportes lógicos (Decretos N° 323/007, 207/007, 150/007 y 148/007).

Adicionalmente, mediante el Decreto N° 174/05 se incorpora al ordenamiento jurídico interno la Resolución N° 17/04 del MERCOSUR, que aprueba la normativa relativa a la informatización del manifiesto internacional de cargas/declaración de tránsito aduanero.

#### b) Protección al consumidor

En cuanto a la protección al consumidor, la Ley de Defensa del Consumidor (Ley N° 17.250) regula de manera somera algunos aspectos sobre las operaciones de comercio en línea, al establecer que la oferta dirigida a consumidores determinados o indeterminados, transmitida por cualquier medio de comunicación y que contenga información suficientemente precisa con relación a los productos o servicios ofrecidos, vincula a quien la emite y a aquel que la utiliza de manera expresa por el tiempo que se realice. De igual forma, dispone que la oferta de productos o servicios que se realice fuera del local empresarial, por medio postal, telefónico, televisivo, informático o similar da derecho al consumidor que la aceptó a rescindir o resolver, "ipso-jure", el contrato dentro de los cinco días hábiles contados desde la formalización del contrato o de la entrega del producto, a su elección y sin responsabilidad alguna de su parte.

Cabe señalar que la Ley N° 17.250 ha sido reglamentada a través del Decreto N° 244/000, del 23 de agosto de 2000, que establece, entre otros puntos, el procedimiento para sustanciar las reclamaciones de los consumidores. Asimismo, en virtud de la Ley N° 18.507, del 26 de junio de 2009, se instrumenta un procedimiento especial para las relaciones de consumo regulados por la Ley N° 17.250, para atender reclamos por montos menores a \$100 pesos uruguayos (US\$ 3,115 dólares norteamericanos, aproximadamente). El procedimiento se sustancia ante los Juzgados de Paz.

En virtud del Decreto N° 246/005, del 8 de agosto de 2005, se incorporó al derecho interno la Resolución N° 21/004 del MERCOSUR que regula "el derecho a la información del consumidor en las transacciones comerciales efectuadas a través de Internet".

#### c) Protección de datos personales

Además de la protección constitucional, se promulgó la Ley de Protección de Datos Personales y Acción de "Hábeas Data" (Ley N° 18.331), del 11 de agosto de 2008, que aplica el modelo de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de Europa relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, cuyo nivel de adecuación ha sido avalado por las autoridades europeas. La Ley reconoce el derecho a la protección de los datos personales como inherente a la personalidad humana, por lo que su ámbito de aplicación subjetivo abarca a las personas físicas, aunque también reconoce la pro-

tección a las personas jurídicas en lo correspondiente. La Ley se aplica a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado.

Reconoce a favor de los titulares de los datos su derecho a la información, al acceso, la rectificación, actualización, inclusión o supresión de sus datos personales, así como su derecho a impugnar la valoración personal basada en el tratamiento automatizado o no de datos y el derecho a limitar la comunicación de sus datos a través de la acción de protección de datos o hábeas data, que se hace valer ante la autoridad judicial en un procedimiento sumario. La Ley desarrolla diversos principios que deben regir el tratamiento de los datos, entre los cuales destacan los siguientes: i) legalidad; ii) veracidad; iii) finalidad; iv) previo consentimiento informado; v) seguridad de los datos; vi) reserva, y vii) responsabilidad.

El órgano de control a cargo de supervisar el cumplimiento de la Ley es la Unidad Reguladora y de Control de Datos Personales (URCDP), órgano desconcentrado de la AGESIC que tiene facultades para hacer valer la Ley.

La Ley prohíbe las transferencias de datos personales de cualquier tipo con países u organismos internacionales que no proporcionen niveles de protección adecuados de acuerdo con los estándares del Derecho Internacional o Regional en la materia. También ordena que toda base de datos pública o privada debe inscribirse en el Registro habilitado por la URCDP. Ningún usuario de datos puede poseer datos personales de naturaleza distinta a los declarados en dicho registro. En caso de infracción a la Ley, la URCDP cuenta con facultades sancionatorias que pueden hacer valer, a través de la imposición de apercibimientos, multas de hasta quinientas mil unidades indexadas, así como la suspensión de la base de datos. En el ámbito de las sanciones penales, la Ley señala que las personas que, por su situación laboral u otra forma de relación con el responsable de una base de datos tuvieren acceso o intervengan en cualquier fase del tratamiento de datos personales, están obligadas a guardar estricto secreto profesional sobre los mismos.

La Ley ha sido reglamentada mediante Decreto Reglamentario N° 414/09, de agosto de 2009, que define con mayores elementos las medidas de seguridad que se deben instrumentar para proteger los datos personales, y abunda sobre los diversos requerimientos para solventar los distintos procesos previstos en la Ley.

#### d) Propiedad industrial e intelectual

En cuanto a la normativa en materia de propiedad intelectual, destaca la Ley de Propiedad Literaria y Artística (Ley N° 9.739), del 17 de diciembre de 1937, modificada por la Ley de Derechos de Autor y Derechos Conexos (Ley N° 17.616), del 17 de enero de 2003, que protege los derechos de los artistas, intérpretes y ejecutantes, productores de fonogramas y organismos de radiodifusión, respecto de sus obras y derechos conexos, dentro de los cuales se reconoce la facultad de enajenar, reproducir, distribuir, publicar, traducir, adaptar, transformar, comunicar o poner a disposición del público las mismas, en cualquier forma o procedimiento.

Adicionalmente, resulta importante la Ley N° 18.253, del 5 de marzo de 2008, que aprueba el Tratado de la Organización Mundial de la Propiedad Intelectual sobre Interpretación o Ejecución y Fonogramas, y Declaraciones concertadas relativas al mismo, así como la Ley N° 18.036, del 31 de octubre de 2006, que aprueba el Tratado de la Organización Mundial de la Propiedad Intelectual sobre Derecho de Autor y Declaraciones concertadas relativas al mismo. En materia de marcas, es preciso mencionar la Ley de Normas Relativas a las Marcas (Ley N° 17.011), aprobada el 7 de octubre de 1998, y la Ley 912/1996, del 27 de junio de 1996, que aprueba el Protocolo de Armonización de Normas sobre la Propiedad Intelectual en el MERCOSUR, en materia de marcas, indicaciones de procedencia y denominaciones de origen, vigente a nivel del MERCOSUR.

#### e) Nombres de dominio

Con respecto a nombres de dominio, el NIC de Uruguay es administrado por el Servicio Central de Informática Universitaria (SeCIU) que depende de la Universidad de la República, por delegación de la Autoridad de Números Asignados en Internet (IANA).

Actualmente el .com.uy es administrado por la Administración Nacional de Telecomunicaciones (ANTEL) por delegación del SeCIU. Las controversias relacionadas con los nombres de dominio .UY se dirimen utilizando el Reglamento de Arbitraje del Centro de Conciliación y Arbitraje, la Corte de Arbitraje Internacional para el MERCOSUR, la Bolsa de Comercio del Uruguay, el cual incluye diversas disposiciones de la Política uniforme de solución de controversias en materia de nombres de dominio de la ICANN.

Cabe señalar, respecto de los nombres de dominio gubernamentales “.gub.uy” y “.mil.uy”, que la AGESIC colabora con el SeCIU en el proceso de registro y renovación de nombres de dominio.

#### f) Delitos Informáticos y Seguridad de la Información

En materia de delitos informáticos no se cuenta con una ley específica, sin embargo, se han incorporado normas que establecen diferentes delitos informáticos. Así pues, la Ley de Presupuesto Nacional (Ley N° 16.736), del 12 de enero de 1996, equipara a los delitos de falsificación de documentos públicos tipificados en el Código Penal la transmisión voluntaria de un texto del que resulte un documento infiel, la adulteración o destrucción de un documento almacenado en soporte magnético, o su respaldo, utilizando medios informáticos y telemáticos. Adicionalmente, la Ley de violencia sexual comercial o no comercial cometida contra niños, adolescentes o incapaces (Ley N° 17.815), del 14 de septiembre de 2004, tipifica como delito el comercio y la difusión de material pornográfico (sin distinguir su formato) en el que aparezca la imagen u otra forma de representación de personas menores de edad o personas incapaces, así como la facilitación (en cualquier modo) de la comercialización y difusión de material pornográfico con la imagen u otra representación de una o más personas menores de edad o incapaces.

Por su parte, la Ley de Atentando contra la regularidad de las telecomunicaciones (Ley N° 18.383), del 31 de octubre de 2008, que modifica el artículo 217 del Código Penal, sanciona con pena privativa de la libertad a quien de cualquier manera atentare contra la regularidad de las telecomunicaciones alámbricas o inalámbricas. Es importante señalar que el Poder Judicial se ha pronunciado sobre distintos delitos en su jurisprudencia, incluyendo aquellos que se vinculan con los fraudes o estafas realizadas por Internet, la piratería de software y la ciberocupación de dominios, entre otros.

Adicionalmente, mediante la Ley N° 18.362, del 15 de octubre de 2008, se crea el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy), que depende de la AGESIC y que tiene por objeto regular la protección de los activos de información críticos del Estado, de acuerdo con los criterios sugeridos por el Consejo Honorario de Seguridad Informática. Mediante el Decreto N° 451/009, del 28 de septiembre de 2009, emitido por la AGESIC, se regula su funcionamiento y organización. Asimismo, es importante mencionar el Decreto N° 452/009, del 28 de septiembre de 2009, emitido por la AGESIC, que regula la adopción de una política de seguridad en informática de los organismos públicos.

#### g) Iniciativas de Ley y retos

Entre las iniciativas de Ley que están en proceso de elaboración, se encuentra el proyecto de ley en ma-

teria de comercio electrónico, a cargo de la AGESIC. Entre los principales retos que enfrenta Uruguay está el tema relativo a los delitos informáticos, cuya legislación precisa de reformas relevantes a efectos de incorporar las disposiciones sustantivas y procesales previstas en el Convenio del Consejo de Europa sobre la Ciberdelincuencia (con independencia de su adhesión a dicho instrumento con el fin de robustecer la cooperación internacional para la investigación y persecución de los delitos informáticos). La AGESIC ha presentado al Parlamento una iniciativa de Ley en materia de delitos informáticos, sujeta a debate parlamentario.

## VENEZUELA

En el Plan Nacional de Ciencia, Tecnología e Innovación 2005-2030: Construyendo un futuro sustentable, Venezuela apuesta por el desarrollo de las TIC, particularmente en el ámbito del gobierno digital, sin incluir de forma expresa una estrategia para fomentar el comercio electrónico. Con la Ley sobre Mensajes de Datos y Firmas Electrónicas, del 13 de diciembre de 2000, la Ley de Infogobierno, del 17 de octubre de 2013, así como las leyes del sector financie o que se describen en los apartados siguientes, se ha dado sustento legal a las operaciones de comercio electrónico.

#### a) Transacciones electrónicas / Firmas electrónicas

En materia de transacciones electrónicas, la Ley sobre Mensajes de Datos y Firmas Electrónicas adopta diversas disposiciones de la Ley Modelo de la CNUDMI sobre Comercio Electrónico y reconoce la eficacia y el valor jurídico de la firma electrónica, los mensajes de datos y de toda información inteligible en formato electrónico, con independencia de su soporte material y de si proviene de personas naturales o jurídicas, públicas o privadas. De igual forma, regula la operación de los Proveedores de Servicios de Certificación (PSC) y los efectos legales de los Certificados Electrónicos.

Adicionalmente, el Reglamento Parcial del Decreto de Ley sobre Mensajes de Datos y Firmas Electrónicas, del 14 de diciembre de 2004, regula con mayor detalle algunos aspectos de la Ley, particularmente los relacionados con la acreditación de los PSC y las facultades de la Superintendencia de Servicios de Certificación Electrónica. Asimismo, establece las reglas que se deben observar para el manejo de los datos de generación de firmas electrónicas, los cuales una vez creados por los PSC, deben ser entregados al signatario de forma personal e inmediata. De igual

forma, establece los estándares, planes y procedimientos de seguridad que deberán seguir los PSC.

Destaca también el Decreto mediante el cual se declara el acceso y el uso de Internet como política prioritaria para el desarrollo cultural, económico, social y político de la República Bolivariana de Venezuela, del 10 de mayo de 2000.

En cuanto a las transacciones financieras, la Ley General de Bancos y otras instituciones financieras, del 3 de noviembre de 2001, regula la Banca Virtual, los Servicios Desmaterializados, el Servicio de Encomienda Electrónica, los Sistemas Electrónicos de Contabilidad, así como los Servicios Financieros Virtuales, definidos como el conjunto de productos y servicios ofrecidos por los bancos, entidades de ahorro y préstamo y demás instituciones financieras, para realizar, por medios electrónicos, magnéticos o mecanismos similares, de manera directa y en tiempo real las operaciones que tradicionalmente suponen la realización de llamadas telefónicas o movilizaciones de los usuarios a las oficinas, sucursales o agencias de la institución. De igual forma, reconoce el valor probatorio de los servicios precitados.

La Ley de Tarjetas de Crédito, Débito, Prepagadas y demás Tarjetas de Financiamiento o Pago Electrónico, del 22 de septiembre de 2008, regula todos los aspectos vinculados con el sistema y operadores, de tarjetas de crédito, débito, prepagadas y demás tarjetas, de financiamiento o pago electrónico, así como su financiamiento y las relaciones entre el emisor, el tarjetahabiente y los negocios afiliados al sistema, con el fin de garantizar el respeto y protección de los derechos de los usuarios de dichos instrumentos de pago, obligando al emisor de tales instrumentos a otorgar información adecuada y no engañosa a los tarjetahabientes.

Adicionalmente, en virtud de la Resolución N° 641.10, del 19 de enero de 2011, emitida por la Superintendencia de las Instituciones del Sector Bancario (SUDEBAN), se establecen las "Normas que Regulan el Uso de los Servicios de Banca Electrónica" efectuados a través de cajeros automáticos, banca móvil, puntos de venta, banca por Internet y Banca Telefónica, para dar sustento a diversas transacciones financieras, incluyendo la domiciliación de servicios, los pagos y las transferencias a terceros, en un entorno seguro a cargo de las Instituciones Bancarias, para proteger a los usuarios contra los fraudes electrónicos. La resolución incluye, entre otras medidas de seguridad, la necesidad de adoptar factores de autenticación múltiples para la protección de datos durante cualquier transacción electrónica.

En el ámbito de las transacciones electrónicas gubernamentales, la Ley Orgánica de la Administración Pública establece que los órganos y entes de la Administración Pública deben utilizar los medios electrónicos, informáticos y telemáticos, para su organización, funcionamiento y su relación con las personas, incluyendo la utilización de páginas web. Los documentos reproducidos en medios electrónicos, informáticos, ópticos o telemáticos gozarán de la misma validez y eficacia que los documentos originales, siempre que se cumplan los requisitos exigidos por ley, y se garantice la autenticidad, integridad e inalterabilidad de la información.

Por su parte, la Ley de Contrataciones Públicas, del 6 de septiembre de 2010, regula la actividad del Estado para la adquisición de bienes, prestación de servicios y ejecución de obras, para preservar el patrimonio público, fortalecer la soberanía, desarrollar la capacidad productiva y asegurar la transparencia de las actuaciones de los órganos del Estado. Entre las modalidades de selección de contratista se incluye el concurso abierto, el concurso cerrado, la consulta de precios y la contratación directa. La Ley regula las especificaciones técnicas en las contrataciones electrónicas, estableciendo como requisito el uso de mensajes de datos y firmas electrónicas.

Merece especial atención la Ley Sobre Acceso e Intercambio Electrónico de Datos, Información y Documentación entre los Órganos y Entes del Estado, del 15 de junio de 2012, que establece las bases y los principios que rigen el acceso e intercambio electrónico de datos, información y documentos entre órganos y entes del Estado, con el fin de garantizar la implementación de un estándar de interoperabilidad que permita a los ciudadanos ejercer su derecho a la información y presentar peticiones de servicios interoperables.

De igual forma, establece la obligación para las entidades de gobierno de desarrollar sistemas de información interoperables y servicios de información bajo estándares abiertos y software libre, así como de utilizar la certificación y la firma electrónica. Faculta a dichas entidades para sustanciar sus actuaciones administrativas por medios electrónicos y a utilizar expedientes electrónicos, así como a digitalizar sus archivos, que deberán firmarse electrónicamente por el funcionario autorizado para realizar copias certificadas en digital. La Ley obliga a los funcionarios a conformar un repositorio digital.

Por su parte, la Ley de Infogobierno, del 17 de octubre de 2013, establece las normas, principios y lineamientos que rigen el uso de las tecnologías de información

libres en los procesos del Estado en sus niveles de gobierno nacional, estatal y municipal, con el objetivo de mejorar la gestión pública, facilitar el acceso de los ciudadanos a la información en sus roles de contralor y usuario, además de promover el desarrollo nacional que garantice la soberanía tecnológica. Promueve la eliminación, simplificación y automatización de los trámites gubernamentales.

La Ley regula distintos temas como los referentes a la Informática forense, las Infraestructuras críticas, la Interoperabilidad, la Seguridad de la información, el Software libre. También faculta a las personas para: i) dirigir peticiones de cualquier tipo mediante el uso de las TIC; ii) realizar pagos, presentar y liquidar impuestos mediante el uso de las TIC; iii) recibir notificaciones por medios electrónicos; iii) acceder a la información pública a través de medios electrónicos seguros, y iv) acceder electrónicamente a los expedientes, entre otros derechos. Asimismo, confiere a los archivos y documentos electrónicos de las entidades gubernamentales con certificación y firmas electrónicas de la misma validez jurídica y eficacia probatoria que los archivos y documentos en formato impreso y con firma autógrafa.

La Ley del Registro Público y del Notariado, del 22 de diciembre de 2006, considera de interés público el uso de medios tecnológicos en la función registral y notarial para que los trámites de recepción, inscripción y publicidad de los documentos sean practicados con celeridad, sin menoscabo de la seguridad jurídica. La Ley ordena que los asientos registrales y la información registral emanada de los soportes electrónicos surtirán todos los efectos jurídicos que corresponden a los documentos públicos. También contempla que todos los soportes físicos del sistema registral y notarial actual se digitalizarán y se transferirán a las bases de datos correspondientes. El proceso registral y notarial podrá ser llevado a cabo íntegramente a partir de documentos electrónicos y se establece que la firma electrónica de los Registradores y Notarios tendrá la misma validez y eficacia probatoria que la Ley otorga a la firma autógrafa

#### b) Protección al consumidor

La Ley Orgánica de Precios Justos, del 23 de enero de 2014, tiene por objeto asegurar el desarrollo armónico, justo, equitativo, productivo y soberano de la economía nacional, a través de la determinación de precios justos de bienes y servicios, mediante el análisis de las estructuras de costos, la fijación del porcentaje máximo de ganancia y la fiscalización efectiva de la actividad económica y comercial; el acceso de las personas a los bienes y servicios para la sa-

tisfacción de sus necesidades; establecer los ilícitos administrativos, sus procedimientos y sanciones, los delitos económicos, su penalización y el resarcimiento de los daños sufridos, para la consolidación del orden económico socialista productivo.

La Ley rige a las actividades económicas realizadas en Venezuela, incluyendo las efectuadas vía medios electrónicos, por personas naturales y jurídicas de derecho público o privado, nacionales o extranjeras, sin embargo, no establece de manera clara las obligaciones que le corresponden a los proveedores y no define expresamente los derechos de los consumidores en línea, como lo hacía la Ley para la Defensa de las Personas en el Acceso a los Bienes y Servicios, del 1 de febrero de 2010, que fue derogada por esta Ley.

Por su parte, la Ley Orgánica de Telecomunicaciones, aprobada el 1 de junio de 2000, obliga a los operadores de servicios de telecomunicaciones a respetar los derechos de los usuarios, entre los que se encuentra el derecho a una información adecuada y no engañosa sobre el contenido y las características de los servicios de Internet, así como la libertad de elección respecto de los prestadores de servicios y el trato equitativo a los consumidores. El incumplimiento de estos deberes es sancionado con multa e incluso, para ciertos casos, la revocación de la habilitación administrativa otorgada para prestar servicios de telecomunicaciones.

La Ley Orgánica para la Protección del Niño y del Adolescente, del 31 de diciembre de 2001, establece medidas preventivas para evitar la producción y venta de juegos computarizados, electrónicos o multimedia que se consideren nocivos para la salud o el desarrollo integral de los niños y adolescentes. De igual forma, prohíbe la exhibición a niños y a adolescentes de materiales en medios multimedia y en redes con contenido pornográfico, o que hagan una apología de la violencia, de los delitos, del uso de tabaco o sustancias alcohólicas, o de estupefacientes.

#### c) Protección de datos personales

En cuanto a la protección de la privacidad y de los datos personales, la Constitución de Venezuela, del 30 de diciembre de 1999, consagra el derecho de toda persona para acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como el derecho a conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos (Hábeas Data), si fuesen erróneos o afectasen ilegítimamente

sus derechos. Asimismo, consagra el derecho de toda persona a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación, previéndose que la Ley limitara el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos.

Por su parte, la Ley para la Defensa de las Personas en el Acceso a los Bienes y Servicios, del 1 de febrero de 2010, ordena que en las negociaciones electrónicas, el proveedor debe garantizar la privacidad y confidencialidad de los datos en las transacciones, a efectos de limitar su acceso únicamente a las personas autorizadas.

La Ley de Infogobierno dispone que la información que conste en los archivos y registros de las entidades gubernamentales son de carácter público, salvo que se trate de información sobre el honor, la vida privada, la intimidad, la propia imagen, la confidencialidad y reputación de las personas y la defensa de la Nación. También faculta a las entidades gubernamentales para recopilar datos de niños, niñas y adolescentes en relación con sus derechos y garantías, previa solicitud de la persona legitimada. La información no puede ser divulgada, cedida, traspasada, ni compartida con ninguna persona natural o jurídica, sin el previo consentimiento de su representante legal, con las excepciones de ley.

Asimismo, dispone que las entidades de gobierno, a través de las TIC, están obligados a notificar a las personas que la información será recolectada de forma automatizada; su propósito, uso y con quién será compartida; las opciones que tienen para ejercer su derecho de acceso, ratificación, supresión y oposición al uso de la referida información y las medidas de seguridad empleadas para proteger dicha información, el registro y archivo, en las bases de datos de los organismos respectivos.

En el ámbito administrativo, la Providencia que establece las Condiciones Generales de las Habilitaciones Administrativas Generales de 2006, dictada por la Comisión Nacional de Telecomunicaciones (CONATEL), señala que los Proveedores de Servicios de Internet tienen el deber de asegurar el secreto y la inviolabilidad de las comunicaciones privadas, así como de adoptar las medidas necesarias para garantizar la protección y confidencialidad de los datos de carácter personal de sus usuarios, absteniéndose de utilizar los datos referidos para fines distintos a la prestación del servicio, salvo en los casos de solicitudes que realicen los órganos de seguridad del Estado u otros organismos

competentes. El incumplimiento de tal deber ocasiona multas y revocatoria de las habilitaciones otorgadas.

#### d) Propiedad industrial e intelectual

En materia de propiedad intelectual, Venezuela ha suscrito la Decisión 486: Régimen Común sobre Propiedad Industrial y la Decisión 351: Régimen Común sobre Derecho de Autor y Derechos Conexos de la Comisión de la Comunidad Andina. Asimismo, se ha adherido al Convenio de Berna y a la Convención de Roma, y ha firmado tanto el Tratado de la OMPI sobre Derecho de Autor (WCT) como el Tratado de la OMPI sobre Interpretación o Ejecución de Fonogramas (WPPT).

A nivel legislativo, la Ley de Propiedad Industrial, del 14 de octubre de 1955, regula los derechos de los inventores, descubridores e introductores sobre las creaciones, inventos o descubrimientos relacionados con la industria; y los de los productores, fabricantes o comerciantes sobre las frases o signos especiales que adopten para distinguir de los similares los resultados de su trabajo o actividad. La Ley confiere a sus titulares el registro de marcas, lemas y denominaciones comerciales, así como de patentes, modelos y dibujos industriales.

Por su parte, la Ley sobre el Derecho de Autor, del 14 de agosto de 1993, protege las obras del ingenio de carácter creador, ya sean de índole literaria, científica o artística, cualquiera que sea su género, forma de expresión, mérito o destino. De igual forma, protege los derechos conexos a los derechos de autor y a las bases de datos, así como los programas de computación, incluida su documentación técnica y manuales de uso.

#### e) Nombres de dominio

Por lo que se refiere a los nombres de dominio, la Comisión Nacional de Telecomunicaciones (CONATEL) administra y gestiona el Centro de Información de Red de la República Bolivariana de Venezuela (NIC.ve), que es la entidad encargada de asignar los nombres de dominio bajo la terminación “.ve” y ha adoptado la Política uniforme de solución de controversias en materia de nombres de dominio, en virtud de la cual las controversias pueden dirimirse ante el Centro de Arbitraje y Mediación de la OMPI.

#### f) Delitos Informáticos y Seguridad de la Información

En materia penal, destaca la Ley Especial Contra los Delitos Informáticos, del 30 de octubre de 2001, que tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, como la prevención y sanción de los delitos cometidos con-

tra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías. Dentro de los delitos tipificados se encuentra el acceso indebido a los sistemas informáticos, el sabotaje o daño a los mismos, el espionaje informático y la falsificación de documentos electrónicos. También sanciona diversos delitos contra la propiedad, particularmente los referidos a la obtención de información perteneciente a terceros para apropiarse de sus bienes o valores, así como el fraude cometido a través del uso de tecnologías de información, el manejo fraudulento de tarjetas inteligentes, la provisión indebida de bienes o servicios y la posesión de equipo para falsificaciones

Adicionalmente, la Ley General de Bancos y otras instituciones financieras, del 3 de noviembre de 2001, incluye dentro de su capítulo de sanciones penales diversos delitos informáticos, entre ellos, la revelación de información confidencial contenida en medios informáticos, el fraude electrónico, la apropiación de información de los clientes, así como la apropiación de información por medios electrónicos.

De igual forma, la Ley Especial Contra los Delitos Informáticos sanciona dentro de los delitos contra niños y adolescentes, el acceso a material pornográfico por parte de los menores, así como la exhibición pornográfica de niños o adolescentes. Por lo que respecta a los delitos contra el orden económico, la Ley castiga la violación de los derechos de propiedad intelectual, así como la violación de los derechos de los consumidores a través de ofertas engañosas.

Cabe mencionar que la Ley establece que los delitos cometidos fuera de Venezuela pueden ser castigados en territorio venezolano cuando hubieren producido efectos en ese país y el responsable no haya sido juzgado por el mismo hecho o evadido el juzgamiento o condenado por tribunales extranjeros.

En materia de seguridad de la información, la Ley de Infogobierno ordena que en las actuaciones electrónicas que realicen las entidades gubernamentales, se debe garantizar la integridad, confidencialidad, autenticidad y disponibilidad de la información, documentos y comunicaciones electrónicas. Asimismo, faculta a la Superintendencia de Servicios de Certificación Electrónica para instrumentar el Sistema Nacional de Protección y Seguridad Informática, integrado por cuatro Subsistemas Nacionales: de Criptografía, de Gestión de Incidentes Telemáticos (VenCERT), de Informática Forense y de Protección de Datos.

#### g) Iniciativas de Ley y retos

Entre los principales retos que enfrenta Venezuela se encuentra el adoptar una legislación general en materia de datos personales, a efectos de cumplir con los compromisos asumidos en la Red Iberoamericana de Protección de Datos. De igual forma, precisa revisar su legislación sustantiva y procesal con el fin de actualizarla, teniendo en cuenta el Convenio del Consejo de Europa sobre la Ciberdelincuencia así como el Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia, y la Recomendación de la COMJIB relativa a la Tipificación y Sanción de la Ciberdelincuencia, de la cual forma parte.

