

# Estado situacional y perspectivas del derecho informático en América Latina y el Caribe

Erick Iriarte Ahon



Septiembre del 2005

Este documento ha sido elaborado por Erick Iriarte Ahon, Director Ejecutivo de Alfa-Redi. El autor agradece la colaboración de José Ovidio Salgueiro de la AVDINT y Andrés Guadamuz González de la Universidad de Edimburgo, quienes revisaron el texto y ayudaron a darle su forma final. Asimismo se agradece los aportes de los miembros de la Comunidad Alfa-Redi quienes proporcionaron información actualizada sobre legislación en América Latina.

Finalmente agradecemos la guía de Martin Hilbert de CEPAL, para la formulación del presente documento, así como su constante apoyo.

Las opiniones expresadas en este documento, que no ha sido sometido a revisión editorial, son de exclusiva responsabilidad del autor y pueden no coincidir con las de las Organizaciones involucradas. Las opiniones expresadas no reflejan la opinión oficial de la Unión Europea.

Publicación de las Naciones Unidas

LC/W.25

Copyright © Naciones Unidas, septiembre del 2005. Todos los derechos reservados  
Impreso en Naciones Unidas, Santiago de Chile.

La autorización para reproducir total o parcialmente esta obra debe solicitarse al Secretario de la Junta de Publicaciones, Sede de las Naciones Unidas, Nueva York, N. Y. 10017, Estados Unidos. Los Estados miembros y sus instituciones gubernamentales pueden reproducir esta obra sin autorización previa. Sólo se les solicita que mencionen la fuente e informen a las Naciones Unidas de tal reproducción.

## Índice

|  |    |
|--|----|
| <b>Resumen</b> .....   | 5  |
| <b>I. Introducción</b> .....   | 7  |
| <b>II. Metodología</b> .....   | 11 |
| <b>III. Diagnósticos</b> .....   | 13 |
| <b>A. Firma electrónica, firma digital y Certificado digital</b> .....       | 13 |
| <b>B. Delitos Informáticos y Delitos cometidos mediante uso de TIC</b> ..... | 17 |
| <b>C. Protección de datos personales y privacidad</b> .....                  | 19 |
| <b>D. Contratación Electrónica</b> .....                                     | 22 |
| <b>IV. Conclusiones y Tareas Pendientes</b> .....                            | 25 |
| <b>V. Hacia agendas subregionales</b> .....                                  | 29 |



## Resumen

Los esfuerzos normativos en los países de América Latina y el Caribe que tratan los asuntos relacionados con la sociedad de la información se han vendido incrementando considerablemente en los últimos años, lo que evidencia que la mayoría de los países finalmente se están preocupando en adecuadamente desarrollar sus sistemas jurídicos para responder a los muchos retos presentados por los cambios tecnológicos de las Tecnologías de la Información y de las Comunicaciones (TIC). Sin embargo, estos cambios muchas veces responden a una fundamental falta de visión y entendimiento de las tecnologías que se intentan regular, lo que significa que muchas veces las legislaciones no cumplen con su objetivo. Este ha llevado a que se promulguen diferentes tipos de legislación que no se adecuan a los verdaderos retos tecnológicos de la sociedad moderna, o que se realizan tan solo copiando soluciones que se han hecho en otros países.

Es fundamental para América Latina y el Caribe el que se piense de manera estructural a la hora de implementar nuevas normas reguladoras de las TIC. A manera de ilustrar estas situaciones, se debe realizar un estudio de lo hecho hasta ahora, de donde se ha fallado, y de las lecciones que se pueden aprender en este respecto.

El presente informe tiene como objetivo primario el establecer un estado situacional de la regulación en diversas áreas de Sociedad de la Información en América Latina y el Caribe, como insumo para el desarrollo de políticas regionales, que sirvan de instrumento de armonización para la diversidad existente o sirvan de fundamento para el desarrollo de normativa en los países donde no exista normativa sobre las áreas analizadas. Con este objetivo en mente, el estudio se centrará en ciertas áreas específicas: Firma Electrónica, Firma Digital y Certificado Digital, Delitos Informáticos y Delitos cometidos mediante el uso de las TIC, Protección de Datos Personales y Privacidad, y, Contratación Electrónica. Estas son las áreas que han sido sujetas a mayores esfuerzos por parte de los entes reguladores en la región, y por ende proveen la mejor opción de realizar un alto en el camino para poder analizar las opciones para el futuro.

Finalmente el informe presenta una identificación de asuntos cruciales a considerar en la fase actual así como los pasos a seguir, basados en las conclusiones y en las tareas pendientes planteadas en el diagnóstico. Se ha buscado una concordancia con la Meta 25 del Plan de Acción sobre Sociedad de la Información en América Latina y el Caribe, eLAC 2007, que solicita “Establecer grupos de trabajo subregionales para promover y fomentar políticas de armonización

de normas y estándares, con el fin de crear marcos legislativos que brinden confianza y seguridad, tanto a nivel nacional como a nivel regional, prestando especial atención a la legislación sobre la protección de la privacidad y datos personales, delitos informáticos y delitos por medio de las TIC, spam, firma electrónica o digital y contratos electrónicos, como marco para el desarrollo de la sociedad de la información”. Los temas propuestos son los de mayor relevancia regional actual, teniendo además como fecha tentativa para iniciar los procesos de armonización en Noviembre del 2005.

Es importante señalar que la propuesta del desarrollo de normativas subregionales implica que si bien existe la necesidad de desarrollar políticas y regulaciones regionales resulta mas sencillo empezar a niveles subregionales y continuar con integraciones entre subregiones guiados por el principio de armonización normativa regional.

## I. Introducción

Desde la aparición de la primera conexión a Internet en América Latina y el Caribe y las primeras delegaciones de números IP<sup>1</sup> para la región, han pasado casi 20 años.<sup>2</sup> Sin embargo el desarrollo explosivo de Internet ha estado marcado por los 10 últimos años con la diseminación de navegadores gráficos y el crecimiento de la world wide web (www). Es también un período en el cual la cantidad de conectados en la región ha aumentado considerablemente, pero aún sigue manteniéndose en un reducido grupo de la población. De acuerdo al Informe de Desarrollo Humano 2004,<sup>3</sup> América Latina y el Caribe tienen aproximadamente 81 usuarios de Internet por cada mil habitantes. Aunque esto es algo mejor al promedio de países en desarrollo (41 usuarios/1000), es todavía muy inferior al promedio de usuarios en los países desarrollados (382 usuarios/1000) y también es inferior al promedio mundial (99.4 usuarios/1000).

Aún con este pequeño grupo de usuarios permanentes los gobiernos empezaron, impulsados por desarrollos en otros países y en documentos de organismos internacionales, una tarea de diseño de normativas en relación al uso de las tecnologías de información y comunicaciones (TIC) y por ende a la Sociedad de la Información.<sup>4</sup> Infelizmente muchos de estos desarrollos normativos no se hicieron armónicamente y muchos de ellos sin basamento en políticas de estado de largo alcance. Este fenómeno sucede primordialmente porque el enfoque de la doctrina y las propuestas de normativas para las TIC en América Latina y el Caribe se ha centrado en el estudio de las tecnologías y las posibles implicaciones jurídicas que estas pueden tener, sin verdaderamente entrar a analizar algunas de las cuestiones fundamentales en este debate ¿Cuál es el rol del derecho con respecto a las innovaciones tecnológicas? ¿Constituye la sociedad de la información un nuevo paradigma que requiera nuevas soluciones jurídicas? ¿Se pueden usar principios legales existentes para analizar y regular la sociedad de la información? Y, si se requieren nuevas soluciones, ¿qué forma deben adquirir?

---

<sup>1</sup> Sigla en inglés de “Internet Protocol”.

<sup>2</sup> De acuerdo con el IANA, la primera delegación de un ccTLD fue en 1987 a Argentina (<http://www.iana.org/root/whois/ar.htm>), siendo que antes de esto se requería estar conectado a Internet.

<sup>3</sup> Proyecto de las Naciones Unidas para el Desarrollo (PNUD), *Informe de Desarrollo Humano 2004*, <http://hdr.undp.org/reports/global/2004/espanol/>.

<sup>4</sup> La sociedad de la información se define generalmente como la relación entre la sociedad y las tecnologías de información, las cuales conllevan un rol crucial en la organización económica de la comunidad. Ver: Castells, Manuel, *The Internet Galaxy*, Oxford: Oxford University Press, 2001, pp.9-36.

Este estudio no pretende responder éstas importantísimas cuestiones, las cuáles han sido analizadas en diversas formas en otros lados mediante excelentes estudios acerca de la regulación en Internet,<sup>5</sup> y sobre la regulación en América Latina y el Caribe, si bien no hay estudios completos, si hay análisis parciales en los diversos artículos publicados en Alfa-Redi.<sup>6</sup> El presente informe tiene como objetivo primario el establecer un primer estado situacional de la regulación en diversas áreas de Sociedad de la Información en América Latina y el Caribe, como insumo para el desarrollo de políticas regionales, que sirvan de instrumento de Desde la aparición de la primera conexión a Internet en América Latina y el Caribe y las primeras delegaciones de números IP<sup>7</sup> para la región, han pasado casi 20 años.<sup>8</sup> Sin embargo el desarrollo explosivo de Internet ha estado marcado por los 10 últimos años con la diseminación de navegadores gráficos y el crecimiento de la world wide web (www). Es también un período en el cual la cantidad de conectados en la región ha aumentado considerablemente, pero aún sigue manteniéndose en un reducido grupo de la población. De acuerdo al Informe de Desarrollo Humano 2004,<sup>9</sup> América Latina y el Caribe tienen aproximadamente 81 usuarios de Internet por cada mil habitantes. Aunque esto es algo mejor al promedio de países en desarrollo (41 usuarios/1000), es todavía muy inferior al promedio de usuarios en los países desarrollados (382 usuarios/1000) y también es inferior al promedio mundial (99.4 usuarios/1000).

Aún con este pequeño grupo de usuarios permanentes los gobiernos empezaron, impulsados por desarrollos en otros países y en documentos de organismos internacionales, una tarea de diseño de normativas en relación al uso de las tecnologías de información y comunicaciones (TIC) y por ende a la Sociedad de la Información.<sup>10</sup> Infelizmente muchos de estos desarrollos normativos no se hicieron armónicamente y muchos de ellos sin basamento en políticas de estado de largo alcance. Este fenómeno sucede primordialmente porque el enfoque de la doctrina y las propuestas de normativas para las TIC en América Latina y el Caribe se ha centrado en el estudio de las tecnologías y las posibles implicaciones jurídicas que estas pueden tener, sin verdaderamente entrar a analizar algunas de las cuestiones fundamentales en este debate ¿Cuál es el rol del derecho con respecto a las innovaciones tecnológicas? ¿Constituye la sociedad de la información un nuevo paradigma que requiera nuevas soluciones jurídicas? ¿Se pueden usar principios legales existentes para analizar y regular la sociedad de la información? Y, si se requieren nuevas soluciones, ¿qué forma deben adquirir?

Este estudio no pretende responder éstas importantísimas cuestiones, las cuáles han sido analizadas en diversas formas en otros lados mediante excelentes estudios acerca de la regulación

---

<sup>5</sup> Algunos estudios que tratan muchas de éstas cuestiones son: Greenleaf, Graham, "An Endnote on Regulating Cyberspace: Architecture vs Law?" 21(2) *University of New South Wales Law Journal* (1998). (<http://www.austlii.edu.au/au/journals/UNSWLJ/1998/52.html>) ; Johnson, David y Post, David, "Law and Borders: The Rise of Law in Cyberspace" 48 *Stanford Law Review* 1367 (1996); Reidenberg, Joel, "Lex Informatica: The Formulation of Information Policy Rules through Technology" 76 *Texas Law Review* 553 (1998).

<sup>6</sup> Alfa-Redi: Revista de Derecho Informático: <http://www.alfa-redi.org/publicacion/>

<sup>7</sup> Sigla en inglés de "Internet Protocol".

<sup>8</sup> De acuerdo con el IANA, la primera delegación de un ccTLD fue en 1987 a Argentina (<http://www.iana.org/root-whois/ar.htm>), siendo que antes de esto se requería estar conectado a Internet.

<sup>9</sup> Proyecto de las Naciones Unidas para el Desarrollo (PNUD), *Informe de Desarrollo Humano 2004*, <http://hdr.undp.org/reports/global/2004/espanol/>.

<sup>10</sup> La sociedad de la información se define generalmente como la relación entre la sociedad y las tecnologías de información, las cuales conllevan un rol crucial en la organización económica de la comunidad. Ver: Castells, Manuel, *The Internet Galaxy*, Oxford: Oxford University Press, 2001, pp.9-36.



en Internet,<sup>11</sup> y sobre la regulación en América Latina y el Caribe, si bien no hay estudios completos, si hay análisis parciales en los diversos artículos publicados en Alfa-Redi.<sup>12</sup> El presente informe tiene como objetivo primario el establecer un primer estado situacional de la regulación en diversas áreas de Sociedad de la Información en América Latina y el Caribe, como insumo para el desarrollo de políticas regionales, que sirvan de instrumento de armonización para la diversidad existente o sirvan de fundamento para el desarrollo de normativa en los países donde no exista normativa sobre las áreas analizadas. Las áreas contempladas son: Firma Electrónica, Firma Digital y Certificado Digital, Delitos Informáticos y Delitos cometidos mediante el uso de las TIC, Protección de Datos Personales y Privacidad, y, Contratación Electrónica.

Es fundamental para el desarrollo de una política regional en torno a la Sociedad de la Información el comprender que la naturaleza extra-territorial inherente al fenómeno social que vivimos requiere de soluciones coordinadas e integradas. Esto puede realizarse al comparar las soluciones ya implementadas con esfuerzos normativos realizados en otras regiones, así como los impulsados por organismos internacionales.

Ciertamente que la Sociedad de la Información es un fenómeno social y, como fenómeno social, requiere una adecuación del derecho (por ende de las normas vigentes), a dicho cambio social. Es en este marco que diversos países en la región han estado desarrollando regulaciones en torno a diversos temas de la Sociedad de la Información, siendo las normas relacionadas a la contratación electrónica (privada y pública) y al comercio electrónico de las primeras que se han desarrollado conjuntamente con las normas sobre firmas digitales; en un siguiente nivel se encuentran las normas relacionadas a validez del documento electrónico y delitos informáticos, habiéndose dejado relegadas, normativas sobre protección de datos personales.

Es importante señalar que muchas experiencias normativas han generado resultados eficaces, que tienen que ser tomados como "best practices" y modelos posibles a seguir, adecuándolo a las realidades propias, sin perder el contexto de una integración subregional y regional, en el principio que la Sociedad de la Información es un fenómeno transfronterizo. Es por ello que será de importancia el trabajo en torno a legislación y jurisdicción aplicable en los casos de hechos que impliquen una diversidad de países en simultáneo.

Es también importante señalar que las normas por si solas no generan un aumento en el uso de las TIC, tampoco las TIC por si solas generan desarrollo social sostenible. Se requiere el diseño y desarrollo de políticas regionales, subregionales y nacionales que utilicen las TIC para el desarrollo. Es pues esta quizás la principal conclusión, que el desarrollo normativo tiene que estar basado en un desarrollo de políticas, de largo plazo, que enmarquen el uso de las normas para el desarrollo.

---

<sup>11</sup> Algunos estudios que tratan muchas de éstas cuestiones son: Greenleaf, Graham, "An Endnote on Regulating Cyberspace: Architecture vs Law?" 21(2) *University of New South Wales Law Journal* (1998). (<http://www.austlii.edu.au/au/journals/UNSWLJ/1998/52.html>) ; Johnson, David y Post, David, "Law and Borders: The Rise of Law in Cyberspace" 48 *Stanford Law Review* 1367 (1996); Reidenberg, Joel, "Lex Informatica: The Formulation of Information Policy Rules through Technology" 76 *Texas Law Review* 553 (1998).

<sup>12</sup> Alfa-Redi: Revista de Derecho Informático: <http://www.alfa-redi.org/publicacion/>



## II. Metodología

Para la recolección de los datos se utilizaron tres mecanismos en simultáneo que dieron la integración de los cuadros presentados. Como primer instrumento se remitió una encuesta temática remitida a alrededor de 6000 personas relacionadas con el quehacer de temas de sociedad de la información, en especial jurídicos, en América Latina y el Caribe, obteniendo 76 respuestas dando información normativa. Las respuestas provinieron de funcionarios gubernamentales, funcionarios de organismos no gubernamentales, investigadores y abogados especializados en regulación de TIC. Como segundo instrumento se utilizó la base de datos de Alfa-Redi,<sup>13</sup> tanto de legislación (la misma que se ha venido desarrollando desde 1999), y se utilizó la base de datos de artículos sobre temas de regulación de la Sociedad de la Información, revisándose alrededor de 750 artículos en búsqueda de las referencias normativas para la región latinoamericana. El tercer instrumento fue la búsqueda normativa directa en las páginas webs de los congresos de los diversos países de la región, enfrentándose a sitios web completamente desactualizados o que no cuentan con servicios de bases de datos normativas, con lo cual hubo que utilizar sitios web referenciales para buscar las normas.<sup>14</sup>

Se espera para una siguiente fase del desarrollo de este monitoreo normativo el poder hacer una indagación a mayor profundidad en las páginas web de organismos públicos relacionados al tema de Sociedad de la Información, en los diversos países de la región; así como contar con un servicio web de acceso a las normas de manera libre, pero que a su vez sirva de instrumento de análisis comparativo.

A manera de comparación, en cada uno de las tablas se incluirá una sección de regulación europea en la materia para poder utilizar un marco jurídico existente que puede servir como ejemplo a seguir en una jurisdicción que ha tenido excelentes resultados a la hora de regular el fenómeno de nuevas tecnologías. Principalmente el estudio de directivas europeas es de gran ayuda porque estas son normativas diseñadas precisamente para armonizar las muchas legislaciones presentes en los países miembros de la Comunidad Europea.

---

<sup>13</sup> <http://www.alfa-redi.org/publicacion/>

<sup>14</sup> Por ejemplo para el tema de Privacidad se trabajó con <http://ulpiano.com> y para nombres de dominio con <http://latinoamericann.org>

Una primera versión de este documento ha sido submetida para evaluación por parte de dos expertos externos, que hicieron comentarios sustantivos, tomando en consideración también los desarrollos del derecho informático de otras regiones, especialmente Europa..<sup>15</sup>

---

<sup>15</sup> Se agradece a José Ovidio Salgueiro A. de Venezuela y Andrés Guadamuz González de Costa Rica por el tiempo y su colaboración. Sin embargo, la responsabilidad sobre el texto es de su autor.

### III. Diagnósticos

#### A. Firma electrónica, firma digital y Certificado digital

De las legislaciones relacionadas a temas de Sociedad de la Información, las referidas a Firma Electrónica/Firma Digital<sup>16</sup> (y por ende a Certificados Digitales), son las que más se han desarrollado en la región, con especial énfasis en los últimos siete años. Es también importante señalar que muchas de las denominadas “Leyes de Comercio Electrónico”, son en realidad leyes de firma electrónica y/o certificados digitales, más que normas de contratación electrónica per se.

Entre los insumos básicos para el desarrollo de la legislación en la región se encuentran la “Ley de Firma Digital de UTAH” (1996), la “Ley Modelo de Comercio Electrónico de UNCITRAL” (1996), La Directiva Europea de Firma Electrónica (1999), la Ley Federal de Firma Digital (Digital Signature Act of 1999) y el desarrollo por parte de UNCITRAL de la “Ley Modelo sobre las Firmas Electrónicas” (2001); sin descontar la labor pionera en la región por parte de Argentina con la normativa sobre firma digital en y para el sector público, y de la “Digital Signature Act” de Puerto Rico.

Si se pudieran agrupar en cierta manera los modelos de regulación, unos van hacia el desarrollo de una Infraestructura de Clave Pública (PKI) con un organismo regulador supra-certificador (que algunos<sup>17</sup> han denominado “Modelo Utah”), frente a un modelo de operación abierta, pero dando un marco de validez y equivalencia tecnológica, sin un organismo regulador supra-estructural, dejando a los usos y costumbres del mercado, un modelo que podemos decir denominar “Abierto”. Argentina, Brasil, Colombia y Venezuela, entre otros, se encuentran entre los primeros y Bermuda, Belice e Islas Cayman, se encuentran entre las que van por el segundo modelo. Existe también un modelo que pretende ser tecnológicamente neutro, y que puede tener o no un ente regulador o certificador. La Directiva Europea de Firma Electrónica se encuentra en este modelo.

---

<sup>16</sup> Es importante el definir estos dos conceptos, ya que pueden generar confusión. Una firma electrónica es cualquier medio electrónico que pueda ser usado para identificar a una persona. Una firma digital es una especie de firma electrónica, pero utiliza métodos criptográficos para asegurar mejor seguridad a la hora de realizar la identificación. Ver: Martínez Nadal, Apolonia, *La Ley de Firma Electrónica*, Madrid: Civitas, 2000, p.38.

<sup>17</sup> Richards, Jason, "The Utah Digital Signature Act As "Model" Legislation: A Critical Analysis", 27(3) *Journal of Computer & Information Law* 873 (1999).

De otro lado, las regulaciones se han desarrollado desde dos perspectivas, por un lado desde el documento digital (y por ende la validación de un documento digital se haría por medio de una firma digital) siendo entonces la regulación de firma una consecuencia, como es el caso de Chile, frente a otras regulaciones que han planteado la regulación desde la firma misma como instrumento para la manifestación de la voluntad, caso de Perú, Brasil o Argentina.

Sea cual sea el camino escogido, la diversidad de definiciones (en base a los posibles modelos e insumos básicos para la creación de las normas), generan dificultades reales a la integración normativa sobre este particular. Es decir, regulaciones de firma electrónica muchas varían entre la estricta regulación de firmas, la validez del documento electrónico, normas sobre manifestación de la voluntad por medios electrónicos y normas sobre contratación electrónica, pero pocas veces se encuentra una legislación que abarca todos estos temas de manera integral. Esto es un problema del que adolecen legislaciones y normativas en este tema en todo el mundo. En los Estados Unidos, se tiene una ley Federal del tema, y cada estado ha tenido que regular al respecto. En la Unión Europea, el tema de firmas electrónicas es tratado tanto en la Directiva de Comercio Electrónico (2000) como en la mencionada Directiva de Firma Electrónica. Sin embargo, esta divergencia puede obedecer al hecho que la tecnología ha variado considerablemente en los últimos diez años, y que esfuerzos iniciales no estaban preparados para tomar en cuenta cambios subsiguientes.

Hay que analizar también que el fenómeno regulador se vio impulsado desde la perspectiva comercial (tanto en temas de comercio-electrónico como el negocio mismo de la certificación digital), por lo cual muchas de las normas relevantes están pensadas en como acreditar a los actores en los procesos de comercio electrónico,<sup>18</sup> como serían las normas de Ecuador y Colombia que son Leyes de Comercio Electrónico, sin que se haya pensado en la firma como un instrumento de la expresión humana, si no únicamente desde la perspectiva en la contratación (las excepciones presentadas en diversas legislaciones de que no se puedan realizar actos “de familia” o “testamentarios” utilizando firmas digitales, por ejemplo, señalan claramente en este sentido).

De la recopilación realizada, el cuadro presentado (Véase Cuadro 1: Firma electrónica, firma digital, certificados digitales), presenta esta diversidad en la regulación de la temática, aunque manteniendo ciertos tópicos comunes a todas. En el caso específico se han priorizado las normas de más alto rango legislativo, entendiendo que son las que dan el marco de desarrollo a las otras.

La mayoría de las legislaciones analizadas presenta una definición de firma digital (en algunos casos denominada también electrónica avanzada), entrelazada con una definición de certificado digital, siendo en la mayoría de los casos requisito para que un documento digital sea completamente aceptado el que la firma se encuentre certificada.

Sobre la Equivalencia Funcional, es decir que la firma sea considerada funcionalmente equivalente a una firma ológrafa, las normas de Puerto Rico, Islas Caimán y Brasil no señalan esta posibilidad. Consideramos que el caso de Brasil es debido a que pudieran encontrarse en otras normas, pero la no presencia en las normas indicadas esta dado también a que en casi su totalidad las normas hablan de equivalencia funcional de los mensajes signados, siendo en sentido estricto equivalencia en relación a los documentos y no a las firmas.

---

<sup>18</sup> Cabe señalar la participación de empresas dedicadas a la certificación digital en diversos proyectos de Ley, como en Argentina y en Perú; pero también la activa participación de organizaciones de impulso al comercio-electrónico en el desarrollo de la regulación. Señalaremos también que la misma perspectiva de UNCITRAL es comercial.

El contenido del certificado digital esta dado por normas mínimas internacionales, sin embargo las legislaciones analizadas presentan una diversidad de tópicos que deben estar presentes en los certificados. Aparte de esto las normas recopiladas de Barbados, Brasil, Ecuador, México y Puerto Rico no presentan indicación sobre que información debe contener el certificado digital. El caso de Ecuador se desarrollo en el reglamento de la Ley. Es de esperar que en las legislaciones del resto de países sea un proceso similar.

Con relación a la posibilidad de utilizar un certificado emitido fuera del país, a excepción de las normas de Belice, Brasil, México y Puerto Rico es factible en todas las otras legislaciones. Ahora bien, hay que indicar que en el caso del Perú originariamente la ley de firmas no contemplaba esta posibilidad y hubo de generar una ley modificatoria solo para incluir esta posibilidad. En el caso de México se considera que la no presencia del tema de validez de certificados emitidos fuera del país es debido a que es una norma que aún no ha sido desarrollada reglamentariamente, pero en el espíritu de la misma se puede entender que se da la posibilidad de esta validez. El caso de Brasil iría en el mismo camino. Una consideración especial son las legislaciones de Belice, Ecuador e Islas Caimán puesto que se incluye la posibilidad de que una firma digital emitida fuera del país pueda ser validada en dichos países.

Argentina, Brasil, Colombia, Ecuador, Panamá, Perú, Puerto Rico, Republica Dominicana y Venezuela presentan regulaciones basadas en infraestructuras de clave públicas con un organismo gubernamental como entidad de acreditación, siendo Brasil, Panamá y Venezuela quienes han establecido un organismos regulador propio para estas temáticas; en el caso Argentino es una función dada a la Secretaría de la Función Pública, en Colombia la Superintendencia de Industria y Comercio, en Ecuador se indico al CONATEL para tener la función, en el Perú fue dado al Instituto Nacional de Defensa de la Competencia y de la Propiedad Intelectual, en Puerto Rico es una función dada al Departamento de Estado y en el caso de República Dominicana es una función dada al Instituto Dominicano de Telecomunicaciones INDOTEL.

Barbados, Belice, Bermudas, Chile, Islas Caimán, México y Uruguay no mencionan, en la legislación analizada, la presencia de un tipo de estructura PKI.<sup>19</sup> Hay que indicar que además en la legislación de Bermuda se indica explícitamente que no se requiere de una autorización previa para realizar labores de certificación, esto a diferencia del resto de países, donde siguiendo las tendencias del PKI se requiere una acreditación a priori para poder otorgar certificados digitales.

Como dato particular es importante señalar la regulación en relación a la temática de la región andina. La firma digital se ha regulado en la región andina en cuatro de los cinco países. En Venezuela se regulo desde la perspectiva de la validación del mensaje de datos; en Colombia y Ecuador están inmersas en la ley de “Comercio Electrónico”, mientras que en Perú el desarrollo normativo estuvo pensado desde la firma como instrumento para la manifestación de la voluntad. Y Bolivia no tiene aún legislación, aunque se encuentra en pleno desarrollo de la misma. Esta diversidad ha generado que los intentos de generar una “armonización normativa” se hayan visto truncados en diversas ocasiones, puesto que los orígenes normativos son dispares. Y aun más las definiciones mismas que utilizan estas cuatro regulaciones son dispares:

*Colombia: Artículo 2°. (...) c) Firma Digital. Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación;*

---

<sup>19</sup> Infraestructura de Clave Pública

Ecuador: Art. 13. *Firma electrónica. Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.*

Perú: Artículo 1. (...) *Entiéndase por firma electrónica a cualquier símbolo avanzado en medios electrónicos, utilizados o adoptado por una parte con intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita. / Artículo 3. La firma digital es aquella firma electrónica que utiliza una técnica de criptografía simétrica basado en el uso de un par de claves único asociada a una clave privada y una clave pública, relacionadas matemáticamente entre sí de tal forma que las personas que conocen la clave pública no pueden derivar de ella la clave privada.*

Venezuela: Artículo 2. (...) *Firma Electrónica: Información creada o utilizada por el Signatario, asociada al Mensaje de Datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado.*

Colombia habla sobre un “valor numérico que se adhiere a un mensaje de datos”, Ecuador indica: “son los datos en forma electrónica consignados en un mensaje de datos”, en Perú se menciona: “cualquier símbolo avanzado en medios electrónicos” y Venezuela dice: “información creada o utilizada por el signatario asociada al mensaje de datos”.

En esencia la firma digital es la misma siempre, tecnológicamente hablando, es por ello que esta diversidad de definiciones (que además comparadas con las otras de la región) también encuentra divergencias semánticas y doctrinales que en esencia generan diversas consecuencias jurídicas. Es decir a diferencia de otras temáticas donde la costumbre social local genera diferencias sobre un mismo tema (al tener puntos de análisis distinto), no es factible entender de diferentes maneras un fenómeno tecnológico (como el de la firma digital).

No se quiere decir que el derecho solamente tiene que aceptar las definiciones tecnológicas y tomarlas como dogma, sino que en aquellos temas que hay ciertos consensos (basados en normas ISO<sup>20</sup> o estándares ITU<sup>21</sup> o normas RFC<sup>22</sup>), no se puede intentar cambiar algo que está definido, puesto que se crean figuras divergentes, que impiden una adecuada acción en procesos sociales que traspasan las fronteras.

Es claro que el no haber contado con una política regional sobre firma digital y haber enfocado el desarrollo de la regulación en el tema de contratación, ha impedido un desarrollo de esquemas de interacción sub-regional, por ejemplo para el intercambio de información por medios digitales con certificación cruzada. Quizás el desarrollo de la normativa boliviana sobre el tema, pueda acoger algún mecanismo que permita el trabajo sub-regional, integrando las normativas existentes, o siendo una suerte de puente entre todas.

---

<sup>20</sup> International Organization for Standardization (<http://www.iso.org>)

<sup>21</sup> international Communication Union (<http://www.itu.int>)

<sup>22</sup> RFC: Request for Comments, documentos base establecidos por la IETF (<http://www.ietf.org>) en relación a Internet



## B. Delitos Informáticos y Delitos cometidos mediante uso de TIC

El análisis internacional y/o regional de los delitos informáticos es de gran dificultad porque por definición, el Derecho Penal es todavía prominentemente un asunto de carácter nacional.<sup>23</sup> A pesar de que existe un creciente movimiento para crear principios de Derecho Penal Internacional,<sup>24</sup> no se ha llegado todavía a desarrollar un concepto internacional de delitos informáticos, por lo que este tema debe ser estudiado por ahora en la forma que se presenta en cada país. Esta situación se hace más clara cuando se toma en cuenta que distintos sistemas jurídicos conllevan diferencias a la hora de criminalizar una acción. En sistemas civiles, para poder tipificar un delito hay que establecer cual es el bien jurídico que la sociedad quiere proteger, y de él desprender cuales serían los hechos punibles, en caso de que dicho bien jurídico sea vulnerado, y establecer por ende cual es la pena por vulnerar dicho bien jurídico. En sistemas de derecho común, no existe codificación de delitos, y los tipos piden hasta ser el resultado de costumbre o jurisprudencia.<sup>25</sup>

La dificultad de poder realizar una sistematización adecuada se evidencia asimismo por la gran diversidad de delitos y bienes jurídicos protegidos. Los Estados Unidos proveen un excelente ejemplo de la gran variedad de delitos relacionados con las TIC. Por ejemplo, existen Estados con diversos delitos que no se encuentran en otros, y hasta ahora se ha criminalizado ciertos tipos de correos basura o Spam.<sup>26</sup> Esto se da mientras en otros países se encuentra la tipificación de prohibir el uso de juegos de computadora en cafés de Internet.<sup>27</sup> El asunto tan complejo que la misma Unión Europea se ha despreocupado casi totalmente del tema de las TIC y el Derecho penal, pero no de manera completa ya que se ha publicado un Convenio sobre Cibercriminalidad, el cual no tiene carácter obligatorio para estados miembros, y tan solo ha sido ratificado por 5 países.<sup>28</sup>

Sin embargo, en medio de esta gran variedad de tipos penales, se pueden empezar a ver algunas tendencias que permiten un limitado análisis comparativo. Inicialmente, se puede decir que existe un creciente número de delitos tipificados que pueden ser utilizados en casos que se relacionen con TIC, pero dependerá de la pericia jurídica en demostrar que las TIC fue el medio mas no el fin en si misma de los delitos. Tal es el caso de difamación, el hecho que sea por medios informáticos no hace que sea otro delito, sino que resultaría que el uso de las TIC configure un agravante o un medio para la realización del delito. Lo mismo ocurriría en el caso de un fraude o delitos de apología del delito. Muchos de estos “delitos mediante medios digitales”, se encontrarían ya tipificados en los códigos penales existentes. En realidad quizás uno de los

---

<sup>23</sup> Ver: Bassiouni, M. Cherif, *International Criminal Law*, 2d ed, Ardsley, N.Y.: Transnational Publisher (1998), pp.4-5.

<sup>24</sup> Para más información acerca de este tema, véase: Sunga, Lyal S. *The emerging system of international criminal law: developments in codification and implementation*, The Hague: Kluwer Law International, (1997); y Ragazzi, Mauricio., *The concept of international obligations erga omnes*, New York: Clarendon Press, 1997.

<sup>25</sup> En varios sistemas de derecho común, el fraude no se encuentra tipificado, si no que es un delito “común”. Véase: Luthy, Teal, "Assigning Common Law Claims for Fraud", 65(3) *University of Chicago Law Review* 1001 (1998).

<sup>26</sup> El CAN-SPAM Act 2003.

<sup>27</sup> Como es el caso de Grecia, véase: Vlaeminck, Philippe y De Wael, Pietr, “The European Union Regulatory Approach of Online Gambling and its Impact on the Global Gaming Industry”, 7(3) *Gaming Law Review* 177 (2003).

<sup>28</sup> Para más detalles acerca de la convención, ver: <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG>

problemas mayores no este en la tipificación de los delitos sino en determinar la legislación y la jurisdicción aplicable (cuando la misma es extra-territorial).

Con el advenimiento de los procesos de Sociedad de la Información, la aparición de nuevos escenarios, nuevas inter-relaciones y nuevas “etiquetas” para las conductas han generado que se trate de regular aquellos actos que vulnerarían derechos. De esta manera apareciera el concepto de *Delitos Informáticos*, que en sentido estricto son aquellos delitos que afectan al bien jurídico “información” (en cualquiera de sus formas: desde mensajes de datos hasta sistemas computacionales); frente a los *Delitos por medios informáticos* que serían una actualización de los delitos ya tipificados pero con un nuevo medio: el tecnológico.

Bajo esta premisa inicial se comenzó a desarrollar las formas de perseguir dichos delitos, y dichas formas, basándose en el principio jurídico de “no hay pena sino hay ley”, requerían la tipificación y explicitación de los hechos delictivos.

En cierta manera los delitos por medios informáticos son variantes de los delitos “clásicos”, por lo cual muchos legisladores optaron por el camino de adecuación normativa, es decir colocar en los artículos pertinentes la acepción: “... y por medios electrónicos”, o similares, Es por ejemplo el caso en el Código Penal de El Salvador o la modificatoria al Código Penal Chileno. En otros casos se planteo la posibilidad de la inclusión de un artículo en la Parte General de los Códigos Penales que sea genérica, indicando que el hecho que sea utilizando alguna TIC agravaría el hecho. Este camino de adecuación normativa afectaba en esencia a un Código Penal ya existente.

Pero las actividades relacionadas a intrusismo informático, sabotaje informático y en general aquellas que afectarán a la información, no se encontrarían contempladas puesto que no encuadran con alguno de los delitos pre-existentes a la irrupción de las TIC. En sentido estricto a estos se les debe denominar Delitos Informáticos. El camino que siguieron los legisladores fue el desarrollo de normas específicas (el caso particular de Venezuela y Chile que son leyes específicas separadas del código penal), el desarrollo de normas específicas que insertaban artículos en el Código Penal, como el caso de Perú, o normas relacionadas que modificaban el Código Penal (el caso de la Ley de Protección de Datos de Argentina o la Ley de Comercio Electrónico de Ecuador).

En el cuadro presentado (Véase Cuadro 2: Delitos Informáticos) se muestra la normativa vigente recolectada en la región en materia de delitos informáticos.

La casi totalidad de las normas presentadas en el cuadro están relacionadas a Delitos Informáticos donde se involucra la información como bien jurídico protegido, y se pena tanto el intrusismo como la alteración/daño de la información.

Con relación a los equipos informáticos, el daño a los mismos es un daño a la propiedad, y aún siendo equipos informáticos una alteración al soporte es un delito utilizando un medio electrónico. Las normas también consideran la posibilidad de hurto o fraude como delitos contra el patrimonio, con el agravante del uso de TIC, como las normas de Costa Rica y Venezuela, así como la del Estado de Sinaloa en México.

La interceptación a las comunicaciones se encuentra contemplada como un delito contra el secreto de las comunicaciones en la mayoría de las legislaciones penales de la región, pero la misma no explícita (en muchos casos por su antigüedad y su no actualización) lo que se refiere a temas de mensajes de datos o correspondencia digital. A nuestro entender la misma si se encontrase protegida porque la legislación esta referida al secreto de las comunicaciones en general y esta claro que los mensajes de datos y la correspondencia digital es una comunicación. Las normas de Ecuador, Costa Rica y Venezuela presentan normativa específica con relación a esta temática.

De otro lado la vulneración esta enfocada en el acceso a datos personales de terceros (entorno de la privacidad de las personas), de modo tal que esta estrechamente ligada a los principios constitucionales y de la Declaración de Derechos Humanos sobre la privacidad de los individuos. La norma de Guatemala esta pensada en la acumulación de datos (en bases de datos) que vulneren la privacidad; mientras que la norma de Argentina, Brasil, Chile, Costa Rica o México estarían enfocados en la eliminación o daño a datos ya obtenidos, e inclusive el ingreso de datos falsos.

Si bien existen diversos proyectos de ley en la región sobre el tema de pornografía y en especial temas de pornografía infantil solo el caso de la norma venezolana es explícita sobre le particular, en tanto Ley, indicando que en el caso de uso de las tecnologías de información en materiales pornográficos se contemplan dos delitos diferentes que son la exhibición de material pornográfico a menores y la utilización de imágenes de menores en material pornográfico conocida como pornografía infantil.

La modificatoria al Código Penal Chileno en lo referente a pornografía infantil incluye el uso de las TIC para cometer estos delitos. Los proyectos en Brasil, Perú, México, entre otros países sobre el particular, que se encuentran en debate legislativo sobre la temática específica también se refieren a los casos de delitos transfronterizos. Es importante señalar que en el caso del Gobierno de la Ciudad de Buenos Aires, diversos municipios de Lima y el Parlamento Peruano se han dado diversas normas en torno al acceso a contenidos pornográficos a menores de edad en ambientes de cabinas públicas/infocentros/telecentros, en una idea de penar el acceso a contenidos pornográficos.

Finalmente cabe destacar que la única norma que abarca todas las temáticas es la “Ley especial contra los Delitos Informáticos” de Venezuela, que también es la única que ve temas de Propiedad Intelectual desde la perspectiva de la vulneración de los derechos intelectuales utilizando medios electrónicos, aunque hay que señalar que las legislaciones sobre derechos de autor y sobre propiedad industrial de la región, así como los países que han firmado los Tratados Internet de la OMPI también tienen normas con relación a la protección de la propiedad intelectual en todos los ámbitos, por ende incluyen el ámbito digital.

## **C. Protección de datos personales y privacidad**

Los conceptos de privacidad y protección de datos personales son un tema pre-existente a la aparición del Internet, y por ende a la aparición de la Sociedad de la Información, sin embargo con las TIC, la automatización y la facilidad de acceso a información, así como los instrumentos para análisis de información cruzada de los individuos, enfrentan a los conceptos clásicos ante nuevos retos.

Los principios de privacidad se encuentran presentes en casi todas las constituciones de la región de una manera explícita, asimismo se encuentran en el Pacto de San José,<sup>29</sup> así como en la Declaración Universal de los Derechos Humanos.<sup>30</sup> Es por esto que no debe sorprender que exista un adecuado tratamiento de la materia en América Latina y el Caribe a nivel legislativo y jurisprudencial.

Es en el área de la privacidad y la protección de datos el ámbito en el que la región ha creado soluciones jurídicas que no tienen paralelo en otras regiones. El Hábeas Data es un recurso

---

<sup>29</sup> Artículo 11.

<sup>30</sup> Artículo 12.

constitucional que defiende la autodeterminación informativa del ciudadano,<sup>31</sup> y es prácticamente un desarrollo que se ah dado tan solo en América Latina y el Caribe. Este derecho constitucional presenta importantes avances en el tema de Habeas Data en la región, que permiten un acercamiento al tema de protección de datos personales, pero falta una adecuada legislación de desarrollo constitucional en los diversos países, que clarifique el modo de empleo y los niveles de protección sobre los datos personales utilizando este instrumento constitucional.

El hecho de encontrarse como preceptos constitucionales, protegidos por instrumentos de garantías constitucionales (como la Acción de Amparo o el Habeas Data), no había permitido que se desarrollara una normativa especializada, por entenderse que se encontraban protegidas a este nivel, pero el fenómeno de la Sociedad de la Información, donde los datos de los individuos son preciados y fácilmente traspasados de un sitio a otro han generado la necesidad de una más compleja solución legislativa en este tema. Es por esta razón que en los últimos años se ha venido desarrollando una nueva generación de legislaciones que siguen el modelo europeo de protección de datos.<sup>32</sup>

La privacidad de la información personal, se ha visto complementada por los principios y normas sobre acceso a la información que pudiera existir en alguna institución pública o privada. De esta manera la legislación de privacidad se concatena con la legislación sobre acceso a la información pública. Es así que la misma acción de Habeas Data pudiera servir para modificar un dato personal en una base de datos, como acceder a información de un organismo gubernamental.

Sumado a lo antes dicho el requerimiento de información necesaria para el desarrollo de mercados económicos sólidos, donde se debe “premiar” al mejor pagador y “castigar” al mal pagador, siendo las denominadas “centrales de información crediticia / centrales de riesgo” instrumentos para determinar las cualidades de un “buen/mal” pagador, generando espacios de acumulación de datos sobre los individuos que debiendo tener una finalidad concreta en algunos casos (por no decir en muchos) han tergiversado su naturaleza.

La armonización regulatoria, también obedece a un requisito para el desarrollo del comercio internacional, es decir que cobra especial relevancia los temas de privacidad y protección de datos, en los marcos de la integración económica. Es el ejemplo del Acuerdo de Asociación económica, concertación política y cooperación entre Chile y la Comunidad Europea,<sup>33</sup> que en su artículo 30, explícitamente habla de la protección de datos. Asimismo en el Acuerdo de Asociación económica, concertación política y cooperación entre la Comunidad Europea y México,<sup>34</sup> se expresa en su artículo 41 en similar camino.

Sin embargo, es necesario que los países del área entiendan que el modelo Europeo no ha resultado inmediatamente en un mejoramiento del acceso a los datos ni en un incremento en la privacidad. Muchos críticos ya han mencionado que en muchos casos, la protección de datos en Europa se encuentra estancada por una creciente burocracia y por falta de interés de los ciudadanos.<sup>35</sup>

Hay que indicar que la temática de la privacidad en entornos digitales y la protección de datos personales ha sido ya contemplada a nivel político por los gobiernos de la región siendo importante señalar lo expresado en la Declaración de la Antigua con motivo del II Encuentro

---

<sup>31</sup> Chirino, Alfredo, *Autodeterminación Informativa y Estado de Derecho en la Sociedad Tecnológica*, San Jose, Costa Rica: Edit CONAMAJ, (1997) p.14.

<sup>32</sup> Guadamuz Andrés, "Habeas Data vs the European Data Protection Directive", 2001(3) *The Journal of Information, Law and Technology* (JILT). [http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001\\_3/guadamuz/](http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_3/guadamuz/).

<sup>33</sup> [https://www.agpd.es/upload/Acuerdo\\_de\\_Asociacion\\_con\\_Chile.pdf](https://www.agpd.es/upload/Acuerdo_de_Asociacion_con_Chile.pdf)

<sup>34</sup> [https://www.agpd.es/upload/Acuerdo\\_de\\_asociacion\\_economica\\_con\\_Mexico.pdf](https://www.agpd.es/upload/Acuerdo_de_asociacion_economica_con_Mexico.pdf)

<sup>35</sup> Edwards, Lilian, ““The Problem with Privacy: A Modest Proposal” 3(3) *Privacy and Data Protection* 6 (2003).

Iberoamericano de Protección de Datos,<sup>36</sup> la Declaración de Cartagena de Indias,<sup>37</sup> y en especial la Declaración de Santa Cruz de la Sierra (Bolivia) con motivo de la XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno<sup>38</sup> que indica:

*“45. Asimismo somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La Antigua por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de nuestra Comunidad.”*

En la región latinoamericana, también se ha ido desarrollando la tendencia de normativas sobre Acceso a la Información Pública, instrumento para incrementar la participación ciudadana en el control de la transparencia de la gestión pública. En muchos casos el mismo instrumento para acceder a la información personal que pudiera estar en una base de datos es utilizada para acceder a información pública, es decir el Habeas Data, aunque se entiende que son dos figuras distintas del acceso a la información, la primera como instrumento de ayuda a la privacidad y en el segundo caso como instrumento de veeduría ciudadana. Es claro que el tema de transparencia de la gestión pública tiene que ser analizado interdependiente de la temática de la privacidad y la protección de datos personales, enfocando en el libre acceso a la información como fundamento de una democracia participativa.

Esta conjunción de situaciones ha generado que la regulación sobre la protección de datos personales se encuentre dispersa, sin una adecuada integración, a excepción clara de Argentina, quien no solo ha dado una legislación explícita sobre protección de datos, sino que la misma ha generado un organismo público dedicado a dar seguimiento a dicha norma. Asimismo dicho organismo esta regulando el uso, transferencia, modificación y acceso a las bases de datos en la actualidad.

Sin embargo Argentina, no es el único país que ha desarrollado legislación en torno a los datos personales. En el cuadro presentado (Véase Cuadro 3: Privacidad y protección de datos personales), se han recopilado y analizado normativas extra-constitucional de Argentina, Brasil, Chile, Ecuador, México, Panamá, Paraguay, Perú y Uruguay.

La presencia de una definición desde el punto de vista económico esta clara en las regulaciones de Paraguay, Perú y Uruguay donde se puede encontrar que la definición de lo que sería un dato está en normas sobre “centrales de riesgo”. Mientras que en Panamá y México se encuentra en la norma sobre acceso a la información pública. Chile y Argentina, tienen normas sobre protección de datos personales. Ni Brasil ni Ecuador dan una definición sobre lo que vendría a ser un dato personal. Pero ahondando en las definiciones, la presencia de definiciones sobre “datos sensibles” se encuentran presentes en las normas de Argentina, Chile, Paraguay y Perú.

En la mayoría de las normas analizadas el derecho al acceso, a la modificación, a la eliminación o a la inclusión de datos personales por parte del titular de los mismos se encuentra presente, incluyendo además conceptos de gratuidad por ejercer dichos derechos, aunque en algunas normas se indica que se pagara el “costo operativo” de dicha acción, tal es el caso de las normas de Argentina, Brasil, Chile, Uruguay. Las normas están referidas a datos personales desprendiéndose de las mismas que se encuentren en bases de datos, pero no se limita a que se encuentren en bases de datos o que estas sean bases informatizadas, sino que afectan datos

<sup>36</sup> <https://www.agpd.es/index.php?idSeccion=345>

<sup>37</sup> <https://www.agpd.es/index.php?idSeccion=409>

<sup>38</sup> <https://www.agpd.es/upload/Declaracion%20Santa%20Cruz%20de%20la%20Sierra%20Bolivia.pdf>

personales que tengan privados o públicos, personas naturales o jurídicas, en bases manuales o informatizadas.

Es de suma importancia entender que en una Sociedad de la Información, donde la circulación de la información personal, y la creación de perfiles de “consumidores/usuarios” es un insumo básico para las acciones “one to one”, las normativas de protección de datos personales deben defender los principios constitucionales y humanos de la privacidad.

Las normas indicadas pudieran entenderse que se relacionan con el tema del SPAM, sobre lo cual existen ciertos proyectos de ley particular. Cuando alguien desea enviar un correo masivo no solicitado lo que hace es tomar un dato personal, en este caso la dirección de email, y acumularla en una base de datos. Si este dato ha sido tomado sin el consentimiento del titular del dato o aún con su consentimiento pero para otra organización, esta base de datos de “correos” estaría violando los principios de la protección de datos personales, por lo cual es perseguible por los instrumentos constitucionales establecidos, como es la acción del Habeas Data.

Sobre el particular Ecuador, en el reglamento de la Ley de Comercio Electrónico y Chile en una norma modificatoria al Código del Consumidor, hablan sobre el SPAM, con relación a como el usuario se pudiera retirar de una base de datos, pero no se habla de la dirección de correo electrónico como dato en si mismo. Venezuela, en su legislación de Protección al Consumidor y al Usuario del 2004 contempla también la figura del SPAM. A la fecha Perú ha emitido una ley sobre el tema, que se encuentra en su fase de desarrollo de reglamento. Un interesante análisis sobre el particular fue elaborado por Claudia Fonseca.<sup>39</sup> Argentina y Colombia se encuentran desarrollando espacios de dialogo abierto sobre la temática, a raíz de iniciativas legislativas.

## D. Contratación Electrónica

Las definiciones de contratación electrónica están relacionadas al medio en donde ocurre una transacción, siendo que la misma es estructuralmente similar a una contratación sin este medio electrónico. Este ha sido uno de los argumentos utilizados por aquellos que consideran que no existe una contratación electrónica, sino simplemente la contratación que ha incorporado un nuevo medio.<sup>40</sup> De esta premisa la regulación en temas de contratación electrónica/comercio electrónico ha tenido dos vertientes fundamentales. La actualización/adecuación de los códigos pre-existentes donde se contemplaba los temas de contratación (códigos civil y/o de comercio), por ejemplo Perú y México; y por otro lado la vertiente de la generación de una legislación especial, por ejemplo Colombia y República Dominicana.

Como aliciente para la segunda vertiente, UNCITRAL desarrolló en 1996 la denominada “Ley Modelo de UNCITRAL sobre Comercio Electrónico”, complementada en 1998 con la “Ley Modelo de UNCITRAL sobre Firmas Electrónicas”. Cabe recabar asimismo que en la Unión Europea el fenómeno de la aceptación de documentos electrónicos ha sido completamente solucionado por la directiva de Comercio Electrónico.

El debate doctrinal en torno a la terminología a utilizar, así como el modelo a aplicar para “actualizar” la legislación de los diversos países, pasaba por la preexistencia del concepto de “firma” o “signación” en muchos de los cuerpos normativos. De esta manera muchas de las legislaciones de comercio-electrónico resultan siendo legislaciones sobre firmas (electrónicas o digitales) y validez de documentos digitales, antes que legislaciones sobre contratación electrónica, en si misma.

---

<sup>39</sup> Monitor sobre Aspectos Jurídicos y Técnicos del SPAM. Alfa-Redi. <http://www.alfa-redi.org/ar-spam>

<sup>40</sup> Véase: Goode, Roy M. *Commercial law in the next millennium: The Hamlyn lectures*, London: Sweet & Maxwell(1998) pp.96-97.

No es que se desconozca la necesidad de tener seguridad en las transacciones, pero en este caso las soluciones técnicas relacionadas no tanto a la firma, sino a la seguridad de las transacciones (en su transmisión), daban y dan mejores resultados, mientras que el fenómeno regulatorio de la firma, al entenderse prioritariamente para el comercio, no ha tenido el auge requerido, puesto que si bien un acto de contratación es un acto jurídico, existen otros actos jurídicos en los cuales la presencia de la firma pudiera ser más relevante.

Pero la necesidad de mejoras en los gobiernos, sobre todo en los temas de compras públicas (ligados a temas de transparencia de la gestión pública), fomentaron el desarrollo de normativa de contratación en el ámbito de las compras públicas, siendo otra tendencia en el desarrollo de la normativa sobre contratación electrónica, aunque enfocada solo a esta temática, como son las normas de Argentina, Chile, Paraguay y Perú citadas.

De esta manera el cuadro presentado (Véase Cuadro 4: Contratación Electrónica / Legislación de Comercio Electrónico / E-procurement), es una muestra de esta diversidad de opciones de regulación.

Las regulaciones más cercanas al modelo de UNCITRAL son las Leyes de Comercio Electrónico de Colombia, República Dominicana y Panamá. La presencia de la “Ley Modelo” es clara en los diversos artículos que componen las normas, más es necesario indicar que a diferencia de la ley modelo que no contaba con una sección de firmas, las tres indicadas han regulado el tema de firmas digitales en sus respectivas leyes.

Ecuador se inspira en las leyes modelo de UNCITRAL, pero realiza un desarrollo sui generis, de mayor profundidad que el caso de Belice que también realiza una norma claramente diseñada para la realidad de los países indicados. Ahora bien, se pueden encontrar referencias a la “ley modelo” en diversos artículos de dichas regulaciones.

Cabe destacar que la Ley de Comercio Electrónico de Ecuador, no solo se enfoca en el tema del documento o la firma, sino que profundiza en temas de Sociedad de la Información, teniendo referencia a Delitos Informáticos así como mecanismos de defensa del consumidor “de servicios de e-commerce”.

Barbados, Bermuda y las Islas Caimán presentan una regulación muy similar, en sus “Electronic Transactions Act”. De hecho la división temática es bastante similar. Dado que la norma de Bermuda es de 1999, asumimos que es de donde tomaron el modelo las otras dos, pero esta norma presenta temáticas específicas de modificación de sus códigos de comercio (en el caso de Caimán y Bermuda), y las tres presentan temas de protección de datos personales sobre las transacciones y de responsabilidad de los proveedores de servicios de e-commerce.

El caso de México es particular puesto que la forma de enfocar la regulación fue por la adecuación de sus códigos vigentes, con modificaciones al código civil, código comercial y código del consumidor. El caso de Perú va en esta línea también al realizar una modificación, en la Ley sobre Manifestación de la Voluntad por Medios Electrónicos, en lo referente a la forma de conocimiento y contratación entre ausentes.

Finalmente el caso de Perú, Chile, Argentina y Colombia en sus normativas sobre Contratación Estatal, han enfocado los procedimientos para las contrataciones públicas estatales, pero hay que destacar que dichas normativas no pueden ir desligadas de normas nacionales propias sobre validez del documento electrónico y sobre firma digital, existentes en dichos países. Esta regulación pues debe estar basada en las de documento y la de firma, y servir de fomento para la contratación electrónica.

Es pues claro que en esencia a excepción de algunos artículos la mayoría de las legislaciones denominadas “leyes de e-commerce” son en realidad leyes sobre firma digital, sobre certificados digitales, sobre entidades de certificación o sobre validez del documento electrónico, antes que sobre contratación electrónica en si misma.





## **IV. Conclusiones y Tareas Pendientes**

### **Conclusiones Preliminares**

Existen diversos niveles, interdependientes e interrelacionados, de regulación con relación a la Sociedad de la Información en América Latina y el Caribe. Un primer nivel de regulación técnica es dada por estándares técnicos (ITU, IETF, ISO) y un segundo nivel de regulación jurídica, basado (o que debería basarse) en dichos estándares técnicos. Sin embargo es en la capa jurídica donde se encuentran conflictos de interpretación de la capa técnica que dan como resultado una diversidad normativa enfocando el mismo fenómeno técnico.

Ciertamente que la Sociedad de la Información es un fenómeno social y, como fenómeno social, requiere una adecuación del derecho (por ende de las normas vigentes), a dicho cambio social. Es en este marco que diversos países en la región han estado desarrollando regulaciones en torno a diversos temas de la Sociedad de la Información, siendo las normas relacionadas a la contratación electrónica (privada y pública) y al comercio electrónico de las primeras que se han desarrollado conjuntamente con las normas sobre firmas electrónicas y firmas digitales; en un siguiente nivel se encuentran las normas relacionadas a validez del documento electrónico y delitos informáticos, habiéndose dejado relegadas, normativas sobre protección de datos personales.

Se ha comprobado en la recopilación normativa la inexistencia de un desarrollo armónico a nivel subregional, mucho menos a nivel regional, motivo por el cual la integración normativa resultará una tarea complicada de realizar, pero que tiene que iniciarse, teniendo por ello ventaja aquellos países que no han desarrollado aún sus normativas, puesto que podrán, basándose en una política regional o subregional, la posibilidad de desarrollar normativa complementaria con el resto de países.

Es importante señalar que existen ejemplos de legislaciones y regulaciones adoptadas en la región que demuestran que por lo menos existe voluntad política de proveer marcos jurídicos a muchos de los fenómenos de la Sociedad de la Información. Es importante mantener el impulso de muchos de estos esfuerzos y poder traducirlos en nuevas leyes que respondan realmente a los retos tecnológicos que enfrenta América Latina y el Caribe. Se debe también tener en cuenta que

es necesario que los legisladores del área se rodeen de asesores que entiendan la tecnología para que las nuevas normativas no adolezcan de pobre entendimiento de la problemática a tratar. Es también importante recordar que otros países y regiones ya han tenido considerable experiencia a la hora de regular las TIC, y que es posible el aprender de los sucesos y fracasos que han experimentado. Esto se puede realizar sin tratar de copiar modelos foráneos de forma ciega, sino analizando las posibles implicaciones de las nuevas normas.

Es también necesario el mantener una saludable dosis de escepticismo tecnológico a la hora de regular. Muy a menudo se trata de pasar una norma reguladora de las TIC sin pensar si se requiere en verdad, sino que tan solo se legisla por el hecho de legislar. Debemos entender que los sistemas jurídicos mundiales han venido evolucionando por milenios, y que muchos fenómenos que creemos vienen a cambiar todo pueden ser perfectamente interpretado con principios de derecho existentes. Es también importante el tomar en cuenta que en algunos temas tecnológicos, cualquier tipo de legislación no tendrá ningún efecto en realidad por la misma naturaleza tecnológica del fenómeno. Los legisladores del área deben intentar concentrar sus esfuerzos para que estos tengan verdadero impacto.

Es también importante señalar que las normas por si solas no generan un aumento en el uso de las TIC, tampoco las TIC por si solas generan desarrollo social sostenible, se requiere el diseño y desarrollo de políticas regionales, subregionales y nacionales que utilicen las TIC para el Desarrollo. Es pues esta quizás la principal conclusión, que el desarrollo normativo tiene que estar basado en un desarrollo de políticas, de largo aliento, que enmarquen el uso de las normas para el desarrollo.

## Tareas Pendientes

### a) Firma Digital

Es de importancia señalar que las tareas pendientes en materia de firma digital, tiene que pensarse como instrumento en el marco de un proceso de uso de firma digital con relación a documentos digitales y su validación (tanto de los primeros como de los segundos) como manifestación de la voluntad. Asimismo deben integrarse en un marco de uso transfronterizo.

*Tarea Pendiente 1:* Integración Normativa subregional y regional por medio de una norma integradora de amplio espectro, que permita incorporar las diferentes perspectivas que se han dado sobre firma digital, facilitando el uso transfronterizo de firmas digitales emitidas en la región, y también de certificados digitales.

*Tarea Pendiente 2:* Análisis sobre uso y aplicación de firma digital en ambientes gubernamentales para el e-government (no solo el e-procurement), es decir uso de firma digital para las actividades cotidianas del ciudadano, en tanto se inter-relaciona con el gobierno, sea para el pago de impuestos, presentación de declaraciones impositivas, solicitudes de documentos (partidas de nacimiento, matrimonio, etc.), presentación de consultas y solicitudes, entre otras actividades.

*Tarea Pendiente 3:* Diseño de mecanismos y manuales de validación cruzada de firmas digitales entre países. Fomento del uso de firma digital en ambientes extra comerciales. Concatenada con la tarea pendiente 1, para una adecuada integración normativa que no empiece de cero, desconociendo las experiencias logradas, deben generarse mecanismos de integración y validación de firmas, fomentando el uso de las mismas no solo para la contratación sino para la manifestación de la voluntad en general.

## b) Delitos Informáticos

A diferencia de otras áreas del Derecho, el Derecho Penal tiene una alta incidencia de las estructuras sociales y culturales propias de cada país. Además el principio jurídico de “no hay pena sin ley previa”, que significa que debe estar correctamente tipificado un delito para poderlo sancionar, hace que las tareas pendientes estén enfocadas a establecer un lenguaje común para poder integrar las propuestas posibles a la normativa local.

*Tarea Pendiente 1:* La regulación existente tiene una confusión terminológica entre lo que son delitos informáticos y delitos por medios electrónicos, siendo tarea fundamental el establecer una adecuada diferenciación y por ende regulación donde se requiera en base a la diferencia conceptual. Asimismo debe ir acompañado del diseño de una propuesta normativa mínima, basada entre otros en las propuestas de tratados de Cybercrime<sup>41</sup> ya existentes.

*Tarea Pendiente 2:* Si una legislación existe en un país y en otro no existe, puede haber problemas cuando los delitos son transfronterizos, como ocurre en el caso de los delitos informáticos y/o delitos por medios electrónicos. Es necesario desarrollar una propuesta regional que permita interactuar a los actores jurídicos de una manera transfronteriza respetando la legislación y jurisdicción propia de cada uno de los países.

*Tarea Pendiente 3:* Se requiere capacitar al poder judicial, cuerpos policiales y de investigación,, y todos aquellos que realizan investigaciones relevantes a causas penales en temas de aspectos legales de Sociedad de la Información, así como formarlos en las herramientas necesarias para combatir estos ilícitos. Es necesario destacar que en algunos países ya existen estas iniciativas (México, Argentina), pero que es necesario el desarrollo de un trabajo colaborativo regional para luchar contra estos delitos.

*Tarea Pendiente 4:* El tema de la pornografía infantil es quizás el delito por medios electrónicos que mas dolor y repudio genera entre los usuarios y no usuarios de la red. Es de especial relevancia la lucha por todos los instrumentos legales existentes, así como la necesidad de implementar herramientas transfronterizas en estos delitos.

## c) Privacidad

*Tarea Pendiente 1:* Fomento de la implementación de Agencias de Protección de Datos (Argentina<sup>42</sup> es el único país que cuenta con este tipo de organización), de un alto nivel en la estructura gubernamental. Estas oficinas deben velar por la adecuada protección de los datos personales, en relación a su uso, manejo, manipulación, traspaso y/o venta. Asimismo debe implementarse una red regional que coordine los esfuerzos de estas Agencias Nacionales. De esta manera es tarea el desarrollo de manuales operativos y de requisitos mínimos para la implementación de dichas oficinas.

*Tarea Pendiente 2:* Es necesario establecer los mínimos necesarios para una adecuada Política y Regulación en Protección de Datos Personales en todos los ámbitos sociales: política, religiosa, económica, cultural, médica, judicial (siendo de especial interés para el último caso la adhesión abierta y aplicación de los Reglas de Heredia).<sup>43</sup> Estos mínimos deben servir de sustento al desarrollo de políticas y normas de protección de datos ínter operables a nivel de los países región. En este mismo sentido el desarrollo de la Red Iberoamericana de Protección de Datos<sup>44</sup>

<sup>41</sup> <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

<sup>42</sup> <http://www.jus.gov.ar/dnmdp/index.html>

<sup>43</sup> <http://www.latinoamericannn.org/ivmundial/gregorio.pdf>

<sup>44</sup> <https://www.agpd.es/index.php?idSeccion=349>

(impulsada por la Agencia de Protección de Datos de España y por la Comunidad Europea), será fundamental para los trabajos en conjunto en la materia.

*Tarea Pendiente 3:* Siendo un subtema específico pero que ha desarrollado implicancias comerciales y sociales especiales, la temática del SPAM tiene que ser considerada en el análisis de políticas y normativas, desde las perspectiva técnica, comercial, jurídica y política, siendo una tarea pendiente el establecer un espacio de monitoreo sobre el particular, así como un trabajo en base a la normativa existente y las propuestas que se puedan realizar, para limitar sino eliminar el SPAM.

#### **d) Contratación Electrónica**

Un hecho notable de la contratación, desde el punto de vista jurídico, es su presencia constante en el devenir humano, siendo quizás una de las temáticas, desde el derecho civil, que más se ha trabajado. Las tareas pendientes están relacionadas a la actualización de los principios jurídicos de la contratación a los nuevos medios tecnológicos, más que a la invención de nuevos principios.

*Tarea Pendiente 1:* Análisis situacional normativo de los códigos civil y de comercio existentes en la región, para la propuesta de normativas de adecuación (caso México, Perú) en temas de contratación electrónica, y manifestación de la voluntad por medios electrónicos. Este análisis debe servir para la propuesta de una norma modelo regional aplicable, de adecuación de los códigos ya existentes.

*Tarea Pendiente 2:* Adecuación de la normativa de contratación gubernamental, especialmente las licitaciones, para que sea posible realizar las compras públicas por medios electrónicos, como instrumento anticorrupción y de mayor acceso a PyMes en los temas de compras públicas, es de especial relevancia estudiar las experiencias ya realizadas en la región y poder utilizarlas de base para fomentar el e-procurement en países que aun no lo implementan.

*Tarea Pendiente 3:* Generar una propuesta regional sobre la contratación electrónica extrafronteriza como compra venta internacional, para lo que se relaciones a temas de jurisdicción y legislación aplicable en la resolución de disputas. Es importante señalar que el desarrollo de soluciones basadas en métodos alternativos de resolución de disputas favorecerá la implementación de normas supra-nacionales.

## **V. Hacia agendas subregionales**

### **A. Región Andina: Firma Electrónica, Firma Digital y Certificado Digital**

La Región Andina posee la Comunidad Andina, organismo que tiene entre sus potestades el desarrollar normativa regional, la misma que al ser puesta en vigencia, es normativa para todos los países de los región, por lo cual el avance en temas de una armonización, pudiera (y debiera) estar pensado desde la perspectiva de una “Decisión Andina” en la temática.

En el reporte de Diagnóstico, la diferencia de definiciones y caminos que han seguido Ecuador, Colombia, Perú y Venezuela en la regulación de la temática, nos permite apreciar que la inexistencia de una política de armonización (y por ende de una normativa armonizada), generarán (cuando ya no lo estén generando) problemas para la integración, no solo comercial, sino de transferencia de documentos digitales.

El hecho que las experiencias comerciales “digitales” no se estén realizando en gran escala al interno de la región, no han permitido apreciar las limitantes de tener legislaciones dispares. Cabe destacar, que en el año 2000 la Comunidad Andina, se planteo la necesidad del desarrollo de una legislación armónica, pero lamentablemente la misma no se pudo desarrollar.

El desarrollo de una legislación armónica, quizás a nivel de “Decisión Andina”, servirá en especial a Bolivia, quien no presenta una legislación sobre la temática, y que no tendría que “adecuar” su normativa a una propuesta regional, sino tomar la “propuesta regional” y hacerla suya.

Como primera acción deberá ser un levantamiento sistematizado de la legislación existente en la subregión andina en temas de firma electrónica, firma digital y certificación electrónica, llegando a los niveles mínimos en los cuales se este aplicando firmas electrónicas o digitales. De esta manera se podrá tener un mapa exacto situacional, y sobre todo tener en claro

los modelos que se han ido implementando en cada país. Esta información servirá de base para el diseño de una propuesta regional integradora.

Ahora bien, siendo que una de las tendencias que se ha seguido en relación a la firma, ha sido su regulación desde la perspectiva del documento digital, es importante que en paralelo al mapeo de regulación de firma se haga lo mismo con la temática del documento electrónico/digital.

Un segundo paso, será por tanto, la armonización de definiciones y la validación fáctica, por medio de una “Decisión Andina”, por un lado en lo referente a validez del documento electrónico y por otro a la “Acreditación Andina para Firmas Electrónicas y/o Digitales” (basados en Certificación Cruzada de Entidades Emisoras), de modo tal que una firma utilizada en cualquiera de los países andinos, sirva de base para cualquier signación de un documento digital en la región. Para este nivel la experiencia de SUSCERTE, será de fundamental ayuda.

Es importante señalar que no debe perderse la perspectiva que la base del desarrollo subregional andino servirá para la implementación de la política y armonización normativa latinoamericana en la temática.

## **B. Centroamérica + Cuba: Delitos Informáticos y Delitos cometidos mediante uso de TIC**

Centroamérica presenta que Costa Rica y Guatemala han desarrollado legislación en la temática, pero dado que el fenómeno de los delitos informáticos y los delitos cometidos mediante uso de TIC tiende a ser transfronterizo, la propuesta del desarrollo de una armonización a nivel regional, va tanto a nivel de desarrollo de legislación (en los países que no la tuvieren) así como en el nivel de capacitación de actores.

La primera fase a desarrollar será el levantamiento de la legislación penal de los diversos países de la subregión, determinando cual de ella es relevante y aplicable, casi siempre a temas de Delitos cometidos mediante uso de TIC. En esta fase también se realizará un mapeo de legislación sobre tema de delitos financieros, sobre todos aquellos relacionados al uso de implementos de tecnología (tales como cajeros automáticos, tarjetas de crédito, etc).

La segunda fase, será el desarrollo de un Acuerdo SubRegional relacionado a jurisdicción aplicable y legislación aplicable en el caso de delitos informáticos o delitos cometidos mediante uso de TIC transfronterizos (dentro de la subregión). Esta propuesta de armonización normativa deberá ir acompañada del diseño de instrumentos para el peritaje forense en temas de TIC.

De esta manera, será fundamental el poder involucrar a la INTERPOL, para generar espacios de capacitación para los actores jurídicos relevantes (jueces, fiscales, policía, abogados, etc.), dado que se debe hacer la transferencia de experiencias de otros países más desarrollados en la temática (en América Latina: Argentina y Colombia), así como de experiencias en Europa.

Un paso en paralelo a la segunda fase, puede ser la adecuación normativa o la firma e implementación del Tratado de Cybercrime,<sup>45</sup> de modo tal que se logre armonizar no solamente a nivel subregional, sino a nivel internacional.

Como tarea pendiente se había indicado el de la pornografía infantil, “(...)es de especial relevancia la lucha por todos los instrumentos legales existentes, así como la necesidad de implementar herramientas transfronterizas en estos delitos.”. Esta lucha debe estar presente

<sup>45</sup> <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

desde un inicio en la propuesta de armonización normativa, puesto que la temática no tiene “tiempo de espera”, pero para la lucha a este nivel se deben establecer los mecanismos jurídicos, judiciales y policiales para poder combatir este flagelo.

### **C. MERCOSUR + Chile: Privacidad y Protección de Datos Personales**

La subregión presenta los mayores avances a nivel regional en temas de Protección de Datos Personales, desde la implementación de la garantía constitucional del Habeas Data en diversas legislaciones hasta el desarrollo de “Agencias de Protección de Datos” como es el caso en Argentina.

La primera fase que se ha de establecer, es un adecuado levantamiento de información subregional sobre la temática, bajando desde las normativas constitucionales, hacia las normativas sectoriales en áreas de salud, educación, trabajo, judiciales, electorales, registros públicos, centrales de información crediticia, entre otras. Será esta fase de levantamiento la más complicada, puesto que habrá que establecer claramente los alcances de las diferentes normas (que se encuentran dispersas y que en el caso de Argentina y Brasil presentan desarrollos Provinciales y Estatales, respectivamente).

La segunda fase será el desarrollo de “Agencias de Protección de Datos” en aquellos países que aún no la posean, siendo el establecimiento de estos organismos, requisitos para poder desarrollar una red subregional de “Entidades de Protección de Datos”, espacio base para el desarrollo de una red regional de la temática.

Hemos de entender que al igual que en otros temas es la protección de la privacidad y la protección de datos personales un tema que muchas veces se transforma en transfronterizo, debiendo establecerse claramente las limitantes para la manipulación/uso/recolección/alteración de los datos personales de los habitantes de la subregión.

En paralelo a la segunda fase de desarrollo deberá acompañarse con el desarrollo de una propuesta de armonización subregional a nivel político y normativo sobre los temas de Acceso a la Información Pública y sobre temas de SPAM, puesto que ambos están ligados a temas de protección de datos personales.

Será de especial relevancia en una tercera etapa el poder trabajar el tema de protección de datos personales a nivel de jurisprudencial, y en general en el entorno judicial, teniendo como base las Reglas de Heredia,<sup>46</sup> de modo tal que se concatene con las propuestas de la Meta 19 del eLAC 2007, sobre la red iberoamericana de e-Justicia.

Es importante señalar que se ha venido trabajando en una Red Iberoamericana de Protección de Datos, liderada por la Agencia Española de Protección de Datos, la misma que debe ser promovida y fomentada.

---

<sup>46</sup> <http://www.latinoamericann.org/ivmundial/gregorio.pdf>

## **D. Caribe + República Dominicana: Contratación Electrónica<sup>47</sup>**

El desarrollo normativo existente en la región Caribe esta influenciada por la Ley Modelo de Comercio Electrónico de UNCITRAL, tal como se puede apreciar en el cuadro presentado en el documento de Diagnóstico.

Este hecho permite avanzar en el mapeo regional, y habrá que determinar los desarrollos sectoriales que se han establecido en materia de contratación electrónica, entre otras en las relaciones empresa-gobierno, en temas de e-procurement.

Como segunda fase se deberá fomentar que los países que aún no cuentan con una legislación en la materia, sea porque no han adoptado la norma de UNCITRAL o porque están esperando una norma subregional, puedan desarrollar sus normativas nacionales enfocadas en los aspectos de la contratación transfronteriza, no siendo limitante la adopción del modelo UNCITRAL, pero si deberá mantener los principios generales de la misma para poder armonizar con la mayoría de países que ya la han implementado en la región caribe.

Es por ello que en paralelo a la segunda fase se deberá analizar el estado situacional de las normativas sobre resolución de disputas, en especial los mecanismos alternativos de resolución de disputas.

Se considera que la *Tarea Pendiente 2* del Diagnóstico, será de especial relevancia, en un proceso que deberá guiarse por lo expresado en las propuestas de metas 10, 11, 13 y 25 del Plan de Acción de eLAC 2007.

Finalmente las normas deberán contemplar los derechos de los consumidores, por lo cual deberá trabajarse armónicamente con la legislación sobre defensa del consumidor ya pre-existente en los países de la subregión.

---

<sup>47</sup> La investigación sobre el Caribe y Republica Dominicana ha sido financiado por trabajos de OSILAC, en cooperación con el ICA-Pan Americas (IDRC).



**Firma Electrónica / Firma Digital / Certificados Digitales**  
**Firma Electrónica o Digital**

| PAÍS/REGIÓN | NORMA/Nº                   | AÑO  | TÍTULO   | Definición   | Ambito de Aplicación  | Equivalencia Funcional | Excepciones | Requisitos para Validez |
|-------------|----------------------------|------|--|--|---|------------------------|-------------|-------------------------|
| Argentina   | Decreto 427                | 1998 | Se aprueba la infraestructura de la Firma Digital para el Sector Público Nacional y se equipara los efectos de la firma digital al de la firma ológrafa                  | Definición (Anexo II): Definición de Firma Dígita  | Artículo 1º   | Artículo 1º            |             | Artículo 5º             |
|             | Ley 25506                  | 2001 | Ley de Firma Digital   | Artículo 2º  | (Aunque no se indica explícitamente es una norma que afecta al sector público y al sector privado). | Artículo 3º            | Artículo 4º | Artículo 9º             |
| Barbados    | Chapter 308B               | 2001 | Electronic Transaction Act   | Section 2.   |   | Section 8.             | Section 3.  |                         |
| Belize      | Chapter 290:01             | 2003 | Electronic Transaction Act   | Section 4.   |   | Section 6.             | Section 15. |                         |
| Bermuda     |                            | 1999 | Electronic Transactions Act  | Section 2.   | Section 6.  | Section 11.            |             |                         |
| Brasil      | Medida Provisória 2.200/01 | 2001 | Insitui a Infra Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências |  |   |                        |             |                         |
|             | Decreto 3587               | 2000 | Estabelece normas para a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal - ICP-Gov, e dá outras providências   | Assinatura Digital. Transformação matemática de uma mensagem por meio da utilização de uma função matemática e da criptografia assimétrica do resultado desta com a chave privada da entidade assinante. |   |                        |             |                         |

|                      |                |      |  |                                 |              |   |             |                          |
|----------------------|----------------|------|--|---------------------------------|--------------|---|-------------|--------------------------|
| Chile                | Ley 19799      | 2002 | Ley sobre Documentos Electrónicos, Firma Electrónica y servicios de Certificación  | Artículo 2º f) y g)             |              | Artículo 3º   | Artículo 3º |                          |
| Colombia             | Ley 527        | 1999 | Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.  | Artículo 2º. c)                 | Artículo 1º. | Artículo 7º   | Artículo 1º | Artículo 28º<br>Párrafo. |
| Ecuador              | Ley 2002-67    | 2002 | Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos   | Artículo 13º                    |              | Artículo 14º  |             | Artículo 15º             |
| Islas Cayman         | Law 7 of 2000  | 2000 | The Electronic Transaction Act   | Section 2.                      |              |   | Section 3.  |                          |
| México               |                | 2000 | Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor. (Artículo 3) |                                 |              | Artículo 3º<br>(...)<br>Modificación<br>al Código de<br>Comercio (...)<br>Artículo 93.- |             |                          |
| Panamá               | Ley 43         | 2001 | Regula los documentos y firmas electrónicas y las entidades de certificación en el comercio electrónico, y el intercambio de documentos electrónicos.  | Artículo 2.5º /<br>Artículo 26º |              | Artículo 7º   | Artículo 7º | Artículo 25º             |
| Perú                 | Ley 27269      | 2000 | Ley de Firmas y Certificados Digitales   | Artículo 1º /<br>Artículo 3º    | Artículo 2.º | Artículo 1º   |             |                          |
| Puerto Rico          | Ley 27310      | 2000 | Ley Modificatoria de la Ley de Firmas y Certificados Digitales   |                                 |              |   |             |                          |
|                      | S.B. 423 (188) | 1998 | Digital Signatures Act   | Section 3. (19)                 |              |   |             |                          |
| República Dominicana | Ley 126-02     | 2002 | Ley sobre Comercio Electrónico, Documentos y Firmas Digitales.   | Artículo 2. i)                  |              | Artículo 6.   |             | Artículo 31.             |

|                   |                  |      |  |                |  |  |               |               |
|-------------------|------------------|------|--|----------------|--|--|---------------|---------------|
| Uruguay           | Decreto 65/998   | 1998 | Reglamenta la implementación de medios electrónicos, de transmisión, almacenamiento y manejo de documentos de la Administración Pública (Capítulo III)   | Artículo 18º   |  |  |               |               |
|                   | Decreto          | 2003 | Reglamenta el uso de la firma digital y el reconocimiento de su eficacia jurídica  | Artículo 2º a) |  |  | Artículo 4º   | Artículo 3º   |
|                   | Ley 17243        | 2000 | Ley considerada con Declaración de Urgencia sobre Servicios Públicos y Privados, Seguridad Pública y Condiciones en las que se desarrollan las actividades productivas (Sección Tercera, artículos 24, 25 y 26 ) |                |  |  | Artículo 25º  |               |
| Venezuela         | Decreto Ley 1204 | 2001 | Ley sobre Mensajes de Datos y Firmas Digitales   | Artículo 2.    |  |  | Artículo 16º  | Artículo 16º  |
| Comunidad Europea | 1999/93/EC       | 1999 | Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica  | Artículo 2.1º  |  |  | Artículo 5.1º | Artículo 2.2º |

*Firma Electrónica / Firma Digital / Certificados Digitales*

**Certificado Digital** **Estructura de PKI**

| PAÍS/REGIÓN | NORMA/Nº                   | AÑO  | TÍTULO  | Validez de Firmas emitidas fuera del país | Definición  | Validez de Certificados emitidos fuera del país | Entidad Licencianta / Autoridad Administrativa   | Entidad Auditante  |
|-------------|----------------------------|------|---|---|---|---|--|--|
| Argentina   | Decreto 427                | 1998 | Se aprueba la infraestructura de la Firma Digital para el Sector Público Nacional y se equipara los efectos de la firma digital al de la firma ológrafa                   |   | Anexo II: Definición de Certificado Digital                                     |   | Secretaría de la Función Pública, dependiente de la Jefatura de Gabinete de Ministros. | Contaduría General de la Nación, dependiente de la Subsecretaría de Presupuesto de la Secretaría de Hacienda del Ministerio de Economía y Obras y Servicios Públicos |
|             | Ley 25506                  | 2001 | Ley de Firma Digital  |   | Artículo 13º  | Artículo 16º                                    | Artículo 29º   | Artículo 27º   |
|             | Chapter 308B               | 2001 | Electronic Transaction Act  |   |   | Section 19.                                     |  | Section 18. (3) and (4)  |
| Belize      | Chapter 290:01             | 2003 | Electronic Transaction Act  | Section 13.                               |   |   |  |  |
| Bermuda     |                            | 1999 | Electronic Transactions Act   |   | Section 2.  | Section 21.                                     | Section 20   |  |
| Brasil      | Medida Provisória 2.200/01 | 2001 | Institui a Infra Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências |   |   |   | Artículo 1º  |  |
|             | Decreto 3587               | 2000 | Estabelece normas para a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal - ICP-Gov, e dá outras providências  |   | Certificado de Chave Pública: Declaração assinada digitalmente por uma AC (...) |   |  |  |

|              |               |      |  |              |                |                 |  |  |
|--------------|---------------|------|--|--------------|----------------|-----------------|--|--|
| Chile        | Ley 19799     | 2002 | Ley sobre Documentos Electrónicos, Firma Electrónica y servicios de Certificación  |              | Artículo 2º b) | Artículo 11º    | Artículo 41º Funciones de la Superintendencia de Industria y Comercio ejercerá las facultades que legalmente le han sido asignadas respecto de las entidades de certificación, (...) |  |
| Colombia     | Ley 527       | 1999 | Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.  |              |                | Artículo 43º    |  |  |
| Ecuador      | Ley 2002-67   | 2002 | Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos   | Artículo 28. | Artículo 20º   | Artículo 28º    | Artículo 37º Organismo de regulación, autorización y registro de las entidades de certificación acreditadas. El Consejo Nacional de Telecomunicaciones "CONATEL" (...)               |  |
| Islas Cayman | Law 7 of 2000 | 2000 | The Electronic Transaction Act   | Section 22.  | Section 2.     | Section 22. (1) |  |  |
| Mexico       |               | 2000 | Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor. (Artículo 3) |              |                |                 |  |  |

|                      |                |      |   |  |                |   |   |  |
|----------------------|----------------|------|---|--|----------------|---|---|--|
| Panama               | Ley 43         | 2001 | Regula los documentos y firmas electrónicas y las entidades de certificación en el comercio electrónico, y el intercambio de documentos electrónicos. |  | Artículo 2. 1º | Artículo 54.                              | Artículo 40º La Autoridad. Se crea dentro del Ministerio de Comercio e Industrias, Dirección de Comercio Electrónico, adscrita a la Dirección Nacional de Comercio, como Autoridad de Registro Voluntario de Prestadores de Servicios de Certificación. La Dirección de Comercio Electrónico establecerá un sistema de acreditación mediante registro voluntario. |  |
|                      |                |      |   |  | Artículo 6º    |   | Artículo 15.º El Poder Ejecutivo, por decreto supremo, determinará la autoridad administrativa competente, señalando sus funciones y facultades. (...)  |  |
| Perú                 | Ley 27269      | 2000 | Ley de Firmas y Certificados Digitales  |  |                |   |   |  |
|                      | Ley 27310      | 2000 | Ley Modificatoria de la Ley de Firmas y Certificados Digitales  |  |                | Modificación Artículo 11º de la Ley 27269 |   |  |
| Puerto Rico          | S.B. 423 (188) | 1998 | Digital Signatures Act  |  | Section 3: (6) |   |   |  |
| República Dominicana | Ley 126-02     | 2002 | Ley sobre Comercio Electrónico, Documentos y Firmas Digitales.  |  | Artículo 2º I) | Artículo 59º                              | Artículo 37º Auditoría a las Entidades de Certificación. El Instituto Dominicano de las Telecomunicaciones (INDOTEL) (...)  | Artículo 37º Auditoría a las Entidades de Certificación. El Instituto Dominicano de las Telecomunicaciones (INDOTEL) (...) |
|                      |                |      |   |  |                |   |   |  |

|                   |                  |      |  |                |               |               |  |  |   |
|-------------------|------------------|------|--|----------------|---------------|---------------|--|--|---|
| Uruguay           | Decreto 65/998   | 1998 | Reglamenta la implementación de medios electrónicos, de transmisión, almacenamiento y manejo de documentos de la Administración Pública (Capítulo III)   | Artículo 2. c) |               |               |  |  |   |
|                   | Decreto          | 2003 | Reglamenta el uso de la firma digital y el reconocimiento de su eficacia jurídica  |                | Artículo 9°   |               |  |  |   |
|                   | Ley 17243        | 2000 | Ley considerada con Declaración de Urgencia sobre Servicios Públicos y Privados, Seguridad Pública y Condiciones en las que se desarrollan las actividades productivas (Sección Tercera, artículos 24, 25 y 26 ) |                |               |               |  |  | Artículo 20° Se crea la Superintendencia de Servicios de Certificación Electrónica, como un servicio autónomo con autonomía presupuestaria, administrativa, financiera y de gestión, en las materias de su competencia, dependiente del Ministerio de Ciencia y Tecnología. |
| Venezuela         | Decreto Ley 1204 | 2001 | Ley sobre Mensajes de Datos y Firmas Digitales   |                | Artículo 2°   | Artículo 45°  |  |  |   |
| Comunidad Europea | 1999/93/EC       | 1999 | Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica  |                | Artículo 2.9° | Artículo 7.1° |  |  |   |

**Delitos Informáticos**  
(*Delitos por medios Informáticos, Delitos Informáticos*)

| PAÍS/REGIÓN | NORMANº   | AÑO  | TÍTULO  | Delitos Informáticos  |  |           |                             | Delitos por medios electrónicos |             |   |  |  |  |
|-------------|-----------|------|---|---|--|-----------|-----------------------------|---------------------------------|-------------|---|--|--|--|
|             |           |      |   | Delitos de daño/alteración de información   | Delitos de intrusismo informático  | Espionaje | Delitos contra la propiedad | Delitos contra la privacidad    | Pornografía | Delitos contra la Propiedad intelectual |  |  |  |
| Argentina   | Ley 25326 | 2000 | Ley de Protección de los Datos Personales (artículo 32)   | Insertar o hacer insertar datos falsos  |  |           |                             |                                 |             |   |  |  |  |
| Brasil      | Ley 9983  | 2000 | Altera o Decreto-lei nº 2.848, de 07 de dezembro de 1940 - Código Penal e dá outras providências. | Insertar datos falsos o no incluir datos / Modificación no autorizada de sistemas de información                  |  |           | -                           |                                 |             |   |  |  |  |
| Chile       | Ley 19223 | 1993 | Ley relativa a Delitos Informáticos   | Destrucción o inutilización de un sistema de tratamiento de información / Alteración, daño o destrucción de datos | Apoderamiento, uso o conocimiento indebido de información contenida en un sistema de tratamiento de información / Revelación o difusión de datos |           |                             |                                 |             |   |  |  |  |



|            |          |      |  |   |  |  |  |   |  |               |  |
|------------|----------|------|--|---|--|--|--|---|--|---------------|--|
|            | Ley 599  | 2000 | Ley que establece el Código Penal (artículo 195)   |   | Acceso abusivo a un sistema informático.                                     |  |  |   |  |               |  |
| Colombia   | Ley 679  | 2001 | Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. |   |  |  |  |   |  | Toda la norma |  |
| Costa Rica | Ley 8148 | 2001 | Que adiciona artículos al Código Penal de Costa Rica para Reprimir y Sancionar Delitos Informáticos  | Acceso, borrar, suprimir, modificar o inutilizar datos registrados en una computadora |  |  |  | Fraude informático  | Violación de comunicaciones electrónicas |               |  |
|            | Ley 8131 | 2001 | De administración financiera de Costa Rica (artículos 110 y 111)   | Obstaculación de ingreso de datos   | Ingreso no autorizado / facilitar a terceros claves de acceso a los sistemas |  |  | Daño a los equipos informáticos de la Administración Financiera |  |               |  |

|                  |                                    |      |  |  |   |  |  |  |
|------------------|------------------------------------|------|--|--|---|--|--|--|
| Ecuador          | Ley 2002-67                        | 2002 | Ley de Comercio Electrónico, Firmas y Mensajes de Datos - Título V | <p>Destrucción o supresión de documentos, información, programas / Alteración de Información en Mensajes de Datos / Destrucción, alteración, inutilización, supresión o daño de información / Apropiación ilícita de sistemas</p> <p>Violentar Claves o Sistemas de Información para acceder u obtener información / Divulgación de Información / obtención y utilización no autorizada de información</p> <p>Divulgación de Secretos Comerciales o Industriales</p> | <p>Destrucción, alteración o inutilización de infraestructura o instalaciones físicas necesarias para transmisión, recepción o procesamiento de</p> <p>Vulneración de la Confiden./ Violación al Derecho a la Intimidad mensajes de datos apropiación ilícita</p> |  |  |  |
| Guatemala        | Decreto 33-96 (artículos 13 al 19) | 1996 | Código Penal - Capítulo VII  | <p>Destruir, borrar o inutilizar registros informáticos / Alterar, borrar o inutilizar instrucciones o programas / Manipulación de Información patrimonial / uso de información / Distribuir poner en circulación programas dañinos que dañen programas o equipos</p> <p>Ingreso no autorizado</p>   | <p>Copia de Programas / Distribuir poner en circulación programas dañinos que dañen programas o equipos</p> <p>Uso o ingreso a una base de datos, sistema o red, para diseñar, ejecutar o alterar un</p>  |  |  |  |
| Mexico / Sinaloa | Decreto 539 (artículo 217)         | 1992 | Código Penal del Estado de Sinaloa - artículo 217                  | <p>Uso o ingreso a una base de datos, sistema o red, para diseñar, ejecutar o alterar un</p>   | <p>Creación de Banco de Datos o registros que afecten la intimidad</p>  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  | esquema para defraudar, obtener dinero, bienes o información / Intercepción, interferencia, recepción, uso, alteración, daño o destrucción de un soporte lógico o programa |  |  |  | esquema para defraudar, obtener dinero, bienes o información |  |  |

|        |           |      |  |  |  |  |  |  |  |                      |
|--------|-----------|------|--|--|--|--|--|--|--|----------------------|
| Mexico |           | 1999 | Código Penal (reforma 1999) - artículo 211   | <p>Modificación, destrucción o pérdida de información sin autorización /</p> <p>Modificación, destrucción o pérdida de información en equipos del Estado sin autorización /</p> <p>Modificación, destrucción o pérdida de información indebida en equipos del Estado /</p> <p>Modificación, destrucción o pérdida de información de entidades del sistema financiero sin autorización /</p> <p>Modificación, destrucción o pérdida de información indebida en equipos del sistema financiero</p> |  |  |  |  |  |                      |
| Peru   | Ley 26612 | 1996 | Modifican el D. Leg N° 681, mediante el cual se regula el uso de tecnologías avanzadas en materia de archivo de documentos e información |  |  |  |  |  |  | Espionaje industrial |

|           |            |      |  |  |  |  |   |   |  |                                      |  |
|-----------|------------|------|--|--|--|--|---|---|--|--------------------------------------|--|
|           | Ley 27309  | 2000 | Ley que Incorpora los Delitos Informáticos al Código Penal | Utiliza, ingresa o interfiere a base de datos, sistema o red de computadoras | Utiliza o ingresa a base de datos, sistema o red de computadoras |  |   |   |  |                                      |  |
| Venezuela | Decreto 48 | 2001 | Ley especial contra los Delitos Informáticos               | Sabotaje o daño a sistemas / Falsificación de documentos                     |  |  | Hurto / Fraude / obtención indebida de servicios o bienes / Manejo fraudulento o apropiación de tarjetas de crédito (o similares) / Oferta Engañosa | Espionaje informático / Violación de la Privacidad o de datos personales / violación de la privacidad de las comunicaciones / revelación indebida de información personal | Difusión o exhibición de material pornográfico / Exhibición pornográfica de niños o adolescentes | Apropiación de Propiedad Intelectual |  |

**Privacidad**  
**(Protección de Datos Personales)**

|                    |                 | <b>Protección de Datos Personales</b> |  |                                       |                                      |   |                       |                    |
|--------------------|-----------------|---------------------------------------|--|---------------------------------------|--------------------------------------|---|-----------------------|--------------------|
|                    |                 | <b>Definiciones</b>                   |  | <b>Sobre Bases de Datos</b>           | <b>Sobre los Datos</b>               |   |                       |                    |
| <b>PAÍS/REGIÓN</b> | <b>NORMA/Nº</b> | <b>AÑO</b>                            | <b>TÍTULO</b>  | <b>Definición de Datos Personales</b> | <b>Definición de Datos Sensibles</b> | <b>Obligaciones de los poseedores de Bases de Datos</b> | <b>Consentimiento</b> | <b>Excepciones</b> |
| Argentina          | Ley 25326       | 2000                                  | Ley de Protección de Datos Personales                                | Artículo 2.                           | Artículo 2.                          | Artículo 3.   | Artículo 5.           | Artículo 7.        |
| Brasil             | Lei 9507        | 1997                                  | Ley Reglamentaria del Habeas Data                                    |                                       |                                      |   |                       |                    |
| Chile              | Ley 19628       | 1999                                  | Ley sobre Protección de la Vida Privada                              | Artículo 2. f)                        | Artículo 2. g)                       |   | Artículo 4.           | Artículo 4.        |
| Ecuador            | Ley 2002-67     | 2002                                  | Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos |                                       |                                      | Artículo 9.   | Artículo 9.           | Artículo 9.        |
|                    |                 | 1997                                  | Ley Orgánica de Control Constitucional. Título II: Habeas Data       |                                       |                                      |   |                       |                    |
| Mexico             |                 | 2002                                  | Ley de Transparencia y Acceso a la Información Pública Gubernamental | Artículo 3. II.                       |                                      |   |                       | Artículo 22.       |

|          |           |      |  |               |                |  |  |
|----------|-----------|------|--|---------------|----------------|--|--|
| Panamá   | Ley 6     | 2002 | Que dicta normas para la transparencia en la gestión pública, establece la acción de Hábeas Data y dicta otras disposiciones.            | Artículo 1.5. |                |  |  |
| Paraguay | Ley 1682  | 2000 | Ley que Reglamenta la Información de carácter privado  |               | Artículo 4.    |  |  |
| Perú     | Ley 27489 | 2001 | Ley que regula las centrales privadas de información de riesgos y de protección al titular de la Información                             |               | Artículo 2. c) |  |  |
|          | Ley 28237 | 2004 | Código Procesal Constitucional. Título IV: Hábeas Data   |               |                |  |  |
| Uruguay  | Ley 17838 | 2004 | Se dictan normas para la protección de Datos Personales a ser utilizados en informes comerciales, y se regula la acción de "Habeas Data" |               |                |  |  |

|                   |                    |      |  |                |               |                |             |                |
|-------------------|--------------------|------|--|----------------|---------------|----------------|-------------|----------------|
| Comunidad Europea | Directiva 95/46/CE | 1995 | Directiva 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 | Artículo 2. a) | Artículo 8.1. | Artículo 18.1. | Artículo 7. | Artículo 13.1. |
|-------------------|--------------------|------|--|----------------|---------------|----------------|-------------|----------------|



**Privacidad**

**(Protección de Datos Personales)**

| PAÍS/REGIÓN | NORMA/Nº    | AÑO  | TÍTULO   | Protección de Datos Personales |   |                                  | Ente Regulador                                       | Habeas Data  |
|-------------|-------------|------|--|--------------------------------|---|----------------------------------|--|--|
|             |             |      |  | Sobre los Datos                | Derechos de los titulares de los datos  | Costo del ejercicio de la acción |  |  |
| Argentina   | Ley 25326   | 2000 | Ley de Protección de Datos Personales                                | Transferencia Internacional    | Artículo 12.  | Artículo 13                      | Dirección Nacional de Protección de Datos Personales | Causales para la procedencia de la acción de Habeas Data |
| Brasil      | Lei 9507    | 1997 | Ley Reglamentaria del Habeas Data                                    |                                | Artículo 4.   | Artículo 21.                     |  | Artículo 33.<br>Artículo 7.                              |
| Chile       | Ley 19628   | 1999 | Ley sobre Protección de la Vida Privada                              |                                | Artículo 12 (Derecho a la Información, Eliminación)<br>Artículo 13 (Derecho a la Modificación, Cancelación o Bloqueo) | Artículo 12                      |  |  |
| Ecuador     | Ley 2002-67 | 2002 | Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos |                                |   |                                  |  |  |
|             |             | 1997 | Ley Orgánica de Control Constitucional. Título II: Habeas Data       |                                |   |                                  |  | Artículo 35.   |

|          |           |      |  |   |   |   |              |      |  |
|----------|-----------|------|--|---|---|---|--------------|------|--|
| México   |           |      | 2002   | Ley de Transparencia y Acceso a la Información Pública Gubernamental                                  |   | Artículo 24 (Acceso) / Artículo 25 (Modificación de Datos)  | Artículo 27  | IFAI |  |
| Panamá   | Ley 6     | 2002 | Que dicta normas para la transparencia en la gestión pública, establece la acción de Hábeas Data y dicta otras disposiciones.            |   | Artículo 3.                                   | Artículo 4.   | Artículo 17. |      |  |
| Paraguay | Ley 1682  | 2000 | Ley que Reglamenta la Información de carácter privado  |   | Artículo 2. (Derecho de Acceso) / Artículo 8. |   |              |      |  |
| Perú     | Ley 27489 | 2001 | Ley que regula las centrales privadas de información de riesgos y de protección al titular de la información                             |   | Artículo 13.                                  |   |              |      |  |
|          | Ley 28237 | 2004 | Código Procesal Constitucional. Título IV: Hábeas Data   |   |   |   | Artículo 61. |      |  |
| Uruguay  | Ley 17838 | 2004 | Se dictan normas para la protección de Datos Personales a ser utilizados en informes comerciales, y se regula la acción de "Habeas Data" | Artículo 14 (Derecho de Acceso) / Artículo 15 (Derecho de Rectificación, actualización o eliminación) | Artículo 13.                                  | Artículo 20.- El Ministerio de Economía y Finanzas actuará como órgano de control en el tratamiento de datos personales (...) | Artículo 12. |      |  |

|                   |                    |      |  |                |              |  |  |
|-------------------|--------------------|------|--|----------------|--------------|--|--|
| Comunidad Europea | Directiva 95/46/CE | 1995 | Directiva 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 | Artículo 25.1. | Artículo 12. | Artículo 28. 1. Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva. |  |
|-------------------|--------------------|------|--|----------------|--------------|--|--|

**Contratación Electrónica**  
(*Legislación de Comercio Electrónico / E-procurement*)

| PAÍS/REGIÓN | NORMA/Nº     | AÑO  | TÍTULO  | UNCITRAL               |  |   | Híbridos  | Modificación de Códigos  |                                  |   |  |
|-------------|--------------|------|---|------------------------|--|---|---|--|----------------------------------|---|--|
|             |              |      |   | Siguen Modelo UNCITRAL | Basados en Modelo UNCITRAL y adecuados a la regulación local | Siguen Modelo de UNCITRAL pero incorporan temas específicos |   | Basamento en Ley Modelo de Firma y de Comercio Electrónico en adición con propuestas propias | Modifican Código Civil existente | Modificación Código Comercial existente | Modificación Código del Consumidor existente |
| Argentina   | Decreto 1023 | 2001 | Regula la contratación Pública Electrónica. (artículos 21 y 22) |                        |  |   |   |  |                                  |   |  |
| Barbados    | Chapter 308B | 2001 | Electronic Transaction Act                                      |                        |  |   | Part I: Preliminary / Part II: Legal requirements respecting electronic records / Part III: Communication of electronic records / Part IV: Certification and Accreditation / Part V: Encryption |  |                                  |   |  |

|         |                |      |   |  |  |  |  |  |   |                           |  |
|---------|----------------|------|---|--|--|--|--|--|---|---------------------------|--|
| Belize  | Chapter 290:01 | 2003 | Electronic Transaction Act  |  |  |  |  |  | Artículo 1 al 25. Inspirados en UNCITRAL pero desarrollo propio<br>Part I: Preliminary /<br>Part II: Legal requirements respecting electronic records /<br>Part III: Communication of electronic records /<br>Part IV: Electronic Signatures / Part V: Encryption / | Amended Section 129 / 133 |  |
| Bermuda |                | 1999 | Electronic Transaction Act  |  |  |  |  |  |   |                           |  |
| Chile   | Ley 19955      | 2004 | Modifica la Ley 19496 sobre protección del derecho de los consumidores. Incorporación de artículos: 3Bis b) / 12A |  |  |  |  |  |   |                           |  |
|         | Ley 19886      | 2003 | Ley de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios.                             |  |  |  |  |  |   |                           |  |

|          |                       |      |   |  |   |  |  |  |  |
|----------|-----------------------|------|---|--|---|--|--|--|--|
| Colombia | Ley 527               | 1999 | Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. | Parte I:<br>Parte General/<br>Parte II:<br>Comercio Electrónico en Materia de Transporte de Mercancías | Parte III:<br>Firmas Digitales, Certificados y Entidades de Certificación |  |  |  |  |
|          | Documento CONPES 3249 | 2003 | Política de contratación pública para un Estado gerencial   |  |   |  |  |  |  |
| Ecuador  | Ley 2002-67           | 2002 | Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos  |  |   |  | Título Preliminar /<br>Título II: De las Firmas Electrónicas, Certificados de Firma Electrónica, Entidades de Certificación de Información, Organismos de Promoción de los Servicios Electrónicos, y de Regulación y Control de las entidades de Certificación Acreditadas /<br>Título III: Capítulo I: De los Servicios Electrónicos;<br>Capítulo II: De la contratación electrónica y telemática |  |  |

|              |               |      |  |  |   |   |   |  |  |  |  |
|--------------|---------------|------|--|--|---|---|---|--|--|--|--|
| Islas Cayman | Law 7 of 2000 | 2000 | The Electronic Transaction Law   | Part 1: Preliminary / Part II: Legal Requirements respecting electronic records / Part III: Formation and validity of Contracts / Part IV: Communications of Electronic Records / Part V: Electronic Signatures / Part VI: Information Security Services Providers | Amended Section 196 / Section 201   |   |   |  |  |  |  |
| Mexico       |               | 2000 | Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor. (Artículo 1 y 3) |  | Modificación art. 1805. Contratación entre ausentes. / art. 1811. Conocimiento y Aceptación entre ausentes.     | Modificación art. 80. Aceptación de Oferta por medios electrónicos / Incorporación del Título II: Del Comercio Electrónico, en el Libro II. | Modificación art. 1. Protección del consumidor en transacciones electrónicas. / Inclusión del Capítulo VIII Bis. De los derechos de los consumidores en las transacciones efectuadas a través del uso de Medios electrónicos. |  |  |  |  |
| Panama       | Ley 43        | 2001 | Regula los documentos y firmas electrónicas y las entidades de certificación en el comercio electrónico, y el intercambio de documentos electrónicos.  | Título I: Comercio Electrónico y Documentos en General   | Título II: Firmas y Certificados Electrónicos. / Título III: Autoridad de Registro y Entidades de Certificación |   |   |  |  |  |  |

|          |          |      |                                |  |  |  |  |  |  |  |
|----------|----------|------|--------------------------------|--|--|--|--|--|--|--|
| Paraguay | Ley 2051 | 2003 | Ley de Contrataciones Públicas |  |  |  |  |  |  |  |
|----------|----------|------|--------------------------------|--|--|--|--|--|--|--|



|                      |                             |      |  |  |  |  |  |   |  |  |  |
|----------------------|-----------------------------|------|--|--|--|--|--|---|--|--|--|
| Perú                 | Ley 27291                   | 2000 | Ley de Manifestación de la Voluntad por Medios Electrónicas (artículo 1)   |  |  |  |  |   | Modificación art. 1374. Sobre conocimiento y contratación entre ausentes |  |  |
|                      | Decreto Supremo 31-2002-PCM | 2002 | Aprueban Lineamientos de Políticas Generales del Desarrollo del Sistema Electrónico de Adquisiciones y Contrataciones del Estado   |  |  |  |  |   |  |  |  |
| República Dominicana |                             |      |  |  |  |  | Título I:<br>Disposiciones Generales /<br>Título II:<br>Aplicación de los Requisitos Jurídicos de los Documentos Digitales y Mensajes de Datos / Título III:<br>Comunicación de Documentos Digitales y Mensajes de Datos |   |  |  |  |
|                      | Ley 126-02                  | 2002 | Ley sobre Comercio Electrónico, Documentos y Firmas Digitales.   |  | Título III, Parte II:<br>Comercio Electrónico en materia de Transporte de Mercancías |  |  | Título IV:<br>Firmas Digitales, Certificados y Entidades de Certificación |  |  |  |
| Comunidad Europea    | Directiva 2000/31/CE        | 2000 | Directiva 2000/31/CE del Parlamento Europeo y Consejo, 8 de junio de 2000, relativa a determin. aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior |  |  |  |  |   |  | SI, aunque la forma de modificación será diferente en cada país miembro. |  |
|                      |                             |      |  |  |  |  |  |   |  |  |  |

**Contratación Electrónica**  
(*Legislación de Comercio Electrónico / E-procurement*)

| PAÍS/REGIÓN | NORMA/Nº       | AÑO  | TÍTULO  | Defensa del Consumidor           |  | E-procurement                                     |         |   | Otros Temas                            |                          |  |
|-------------|----------------|------|---|----------------------------------|--|---|---------|---|--|--------------------------|--|
|             |                |      |   | Derecho del Usuario / Consumidor |  | Normativa sobre Compras Públicas                  | Delitos | Protección de Datos                     | Proveedores de Servicios de E-commerce |                          |  |
| Argentina   | Decreto 1023   | 2001 | Regula la contratación Pública Electrónica. (artículos 21 y 22) |                                  |  | Capítulo II: Contrataciones Públicas Electrónicas |         |   |  |                          |  |
| Barbados    | Chapter 308B   | 2001 | Electronic Transaction Act                                      |                                  |  |   |         | Part VI: Protection of Data and Privacy | Part VII: Intermediaries               |                          |  |
| Belize      | Chapter 290:01 | 2003 | Electronic Transaction Act                                      | Artículo 24. Consumer Protection |  |   |         |   |  |                          |  |
| Bermuda     |                | 1999 | Electronic Transaction Act                                      |                                  |  |   |         |   |  | Part VI: Data Protection | Part VII: Intermediaries and E-commerce Services Providers |

|          |                       |      |   |  |  |  |  |  |  |
|----------|-----------------------|------|---|--|--|--|--|--|--|
| Chile    | Ley 19955             | 2004 | Modifica la Ley 19496 sobre protección del derecho de los consumidores. Incorporación de artículos: 3Bis b) / 12A   | Artículo 3BIS b) / (...) Artículo 12A. |  |  |  |  |  |
|          | Ley 19886             | 2003 | Ley de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios.   |  | Capítulo IV: De las compras y contrataciones por medios electrónicos y del sistema de información de las compras y contrataciones de los organismos públicos |  |  |  |  |
| Colombia | Ley 527               | 1999 | Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. |  |  |  |  |  | Sobre desarrollo del Sistema Integral de Contratación Electrónica - SICE |
|          | Documento CONPES 3249 | 2003 | Política de contratación pública para un Estado gerencial   |  |  |  |  |  |  |

|              |               |      |  |  |  |  |                            |  |
|--------------|---------------|------|--|--|--|--|----------------------------|--|
| Ecuador      | Ley 2002-67   | 2002 | Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos   | Título III: Capítulo III: De los derechos de los usuarios o Consumidores de Servicios Electrónicos |  | Título V: De las Infracciones Informáticas                 |                            |  |
| Islas Cayman | Law 7 of 2000 | 2000 | The Electronic Transaction Law   |  |  | Part VII: Intermediaries and E-commerce Services Providers | Part VIII: Data Protection |  |
| Mexico       |               |      | Decreto por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor. (Artículo 1 y 3) |  |  |  |                            |  |
| Panama       | Ley 43        | 2001 | Regula los documentos y firmas electrónicas y las entidades de certificación en el comercio electrónico, y el intercambio de documentos electrónicos.  |  |  |  |                            |  |

|                      |                             |      |  |              |   |  |  |             |
|----------------------|-----------------------------|------|--|--------------|---|--|--|-------------|
| Paraguay             | Ley 2051                    | 2003 | Ley de Contrataciones Públicas   |              | Título V: Sistema de Información de las Contrataciones Públicas (SICP)  |  |  |             |
|                      | Ley 27291                   | 2000 | Ley de Manifestación de la Voluntad por Medios Electrónicas (artículo 1)   |              |   |  |  |             |
| Perú                 | Decreto Supremo 31-2002-PCM | 2002 | Aprueban Lineamientos de Políticas Generales del Desarrollo del Sistema Electrónico de Adquisiciones y Contrataciones del Estado   |              | Sistema Electrónico de Adquisiciones y Contrataciones del Estado / Capacitación a proveedores y servidores públicos |  |  |             |
| República Dominicana | Ley 126-02                  | 2002 | Ley sobre Comercio Electrónico, Documentos y Firmas Digitales.   |              |   |  |  |             |
| Comunidad Europea    | Directiva 2000/31/CE        | 2000 | Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior | Artículo 11. |   |  |  | Artículo 7. |