Panorama del derecho informático en América Latina y el Caribe

Jacopo Gamba

Comisión Económica para América Latina y el Caribe (CEPAL)

Se agradecen los comentarios de Fernando Rojas, Valeria Jordán y Martha Sánchez de la División de Desarrollo Productivo y Empresarial de CEPAL.

Este documento se ha realizado con ayuda financiera de la Unión Europea. Las opiniones expresadas en el mismo no reflejan necesariamente la opinión oficial de la Unión Europea.

Este documento puede ser descargado en línea en http://www.cepal.org/SocInfo.

LC/W.302

Impreso en Naciones Unidas, Santiago de Chile

Índice

I. Introducción

Tradicionalmente, el Derecho y las Tecnologías de Información y Comunicaciones (TIC) pertenecían a dos materias distintas, siendo resumidamente el primero una disciplina que estudia la regulación de la conducta humana en la sociedad, y las segundas un conjunto de servicios, redes, aplicaciones y herramientas tecnológicas cuya incorporación en las actividades del quehacer productivo y social, redunda en la mejora de la calidad de vida de las personas.

Sin embargo, debido al importante avance tecnológico de los últimos años, las TIC se han insertado en muchos ámbitos y actividades, siendo uno de ellos precisamente el del Derecho. Al respecto, es importante destacar que estas materias presentan dos tipos de relaciones:

- Si se toma como enfoque el aspecto meramente instrumental, se está haciendo referencia a la informática jurídica[1], que es la ciencia que estudia la utilización de aparatos o elementos físicos electrónicos, como la computadora, en el Derecho; es decir, la ayuda que este uso presta al desarrollo y aplicación del Derecho. En otras palabras, se trata de analizar **el aspecto instrumental** que surge de la aplicación de la informática en el Derecho.
- Por otro lado, si se considera a la informática como **objeto del Derecho**, o sea como conjunto de procedimientos que la ley tiene que regular, se hace alusión al Derecho de la Informática[2] o simplemente Derecho Informático[3]. En este caso se habla entonces del conjunto de normas, aplicaciones, procesos y relaciones jurídicas que surgen como consecuencia de la aplicación y desarrollo de la informática en diversos aspectos de las relaciones inherentes a las actividades realizadas por los distintos agentes que conforman la sociedad[4].

Como antecedentes al respecto, puede mencionarse que desde que la informatización empezó a dar los primeros pasos comerciales en la década de los 60 y 70 del siglo pasado, se empezaron a desarrollar soluciones informáticas aplicadas al sector de la justicia, tomando forma así lo que hoy se conoce como informática jurídica.

---

1 http://www.informatica-juridica.com/Index.asp

2 Código de Derecho Informático y de Las Nuevas Tecnologías, Gonzalo F. Gallego Higueras, Civitas, Madrid 2002.

3 Para un interesante recorrido entre las definiciones y proveniencia de este concepto véase: Juan Carlos Ríofrio Martínez-Villalba**,** La Pretendida Autonomía del Derecho Informático, 2002.

4 Altmark, Daniel Ricardo, *Informática y Derecho*, vol. 1, Depalma, Buenos Aires, 1987, utilizó una definición diferente: "*conjunto de normas, principios e instituciones que regulan las relaciones jurídicas emergentes de la actividad informática"*.

Al respecto, es pertinente destacar que el primer contacto entre Derecho e Informática inicialmente limitó su enfoque al uso de las tecnologías para el mero almacenamiento de datos legales. Sin ser exhaustivos, se pueden identificar por lo menos tres etapas en este sentido. La primera, situada en los años 60-70, se dirigió a la construcción de bases de datos jurídicas a nivel de la administración pública. En la segunda etapa, años 80-90, la difusión de las computadoras (como dice su nombre, *"personal computer"*), permitió el uso individual de la tecnología para la recolección y la redacción de textos jurídicos: la tecnología entró en el mundo privado de los bufetes de abogados y jueces que escriben textos legales. En una tercera etapa, finales de los 90 en adelante, domina el uso de Internet. En esta etapa la difusión de tecnologías aplicadas al uso diario del derecho es global y permite intercambiar propuestas, contratos, documentos legales, etc., llegando a ser un recurso para el mismo gobierno electrónico, visto en términos generales como el uso de las TIC por parte del sector público con el fin de mejorar los servicios y aumentar la transparencia y la "*accountability*" de los gobiernos.

En América Latina, desde comienzos de los años 70 se empezó a hablar de informática jurídica en la literatura (Anselmo Martino, Antonio Millé, Fernando Jordán Florez). Ya para los años 80 se empezó a manejar difusamente el término y conceptos del Derecho Informático, y a comienzos de los 90 a hacerse realidad la presencia de la informática en la justicia, ya sea mediante Sistemas de seguimiento de casos, también conocidos como "*Tracking Systems*", de manejo de jurisprudencia en sistema documentales y de sistemas para el manejo de estadísticas, entre otros.

En muchos de estos temas, el impacto de las TIC pasa por las decisiones de los gobiernos, en impulsar la aplicación de nuevas tecnologías, lo que ha conllevado que estos procesos de decisión se transformen en un mecanismo lento y difícil, sobre todo en la Región, donde a pesar de los esfuerzos, faltan los recursos necesarios para realizar estos cambios. Los gobiernos han optado por invertir en otras áreas cuyas necesidades son más "visibles", enfocándose en problemas más urgentes. En este complejo panorama, la falta de recursos ha jugado y sigue jugando un papel determinante, no solo en términos económicos sino también humanos, hecho que sigue limitando las iniciativas de la Región en esta materia.

No obstante estas dificultades, a nivel global, en la década de los 90 se ha dado mayor énfasis e importancia a la temática, ya sea tanto de parte de la sociedad civil, como de parte de los gobiernos. Muchas de las legislaciones de la Región que han empezado a ocuparse de comercio electrónico trataban de referirse a normativas de otros países, cuya producción legislativa era más avanzada. Sobre el particular, han jugado un papel importante los esfuerzos de las Naciones Unidas, que con la *United Nations Conference on Trade and Development* (UNCTAD) introdujeron en los años 90 algunas "*Model Laws*" en este ámbito. En otras palabras, en la mayoría de los casos, los países han empezado a enfrentar esta temática evitando crear normas especiales, que necesitan de un conjunto complejo de reformas legislativas, y han preferido utilizar el concepto de *referencia o analogía* a normativas estándar.

En cuanto a los desafíos de la Región en este ámbito, en ocasión del monitoreo del eLAC2007, se ha hecho constar cuales deberían ser los próximos pasos en materia de marco legislativo[5]. Ya sea en materia de firmas electrónicas, o de delitos informáticos, el documento sugiere un mayor esfuerzo de los gobiernos en producir una legislación puntual, en crear capacitación para el perseguimiento de los delitos informáticos y en capacitar a los sistemas judiciales para que estén preparados en enfrentarse con tipologías de crímenes *con* y *en* las TIC. Sin embargo, en la actualidad se observan diversos problemas en la puesta en práctica de tal legislación. Estas dificultades se asocian a la falta de formación en la materia por parte de los diferentes actores del aparato judicial (jueces, fiscales, abogados) y de las fuerzas de la ley para el adecuado peritaje forense.

De esta manera, el propósito de este documento es presentar una recopilación de la reglamentación en vigencia y una descripción de buenas prácticas que permitan tener un panorama de la normativa existente en la Región. En ese sentido, se abordarán las principales y más relevantes temáticas en materia de Derecho Electrónico, que son: firmas y comercio electrónico, gobierno electrónico y transparencia, delitos informáticos y finalmente la e-justicia o aplicación de las TIC a los sistemas judiciales.

[5] CEPAL, *Monitoring eLAC2007: progress and current state of development of Latin American and Caribbean information societies*, Pág. 131.

Este último argumento es relativamente novedoso y aborda un ámbito avanzado de aplicación de las TIC, que representa una evolución de algunos servicios de gobierno electrónico en materia judicial. La Región, en esta esfera, demuestra generalmente iniciativas valiosas y aplicaciones de vanguardia, aunque queden limitadas a algunos sectores judiciales. Algunos países están avanzando mucho más rápidamente respecto a otros y, gracias a sus buenas practicas, pueden ser motor de las reformas necesarias para la informatización de la justicia en la Región.

Los datos presentados en este documento han sido analizados y renovados como corresponde hasta julio 2009.

II. Firma electrónica, contrataciones electrónicas y comercio electrónico

Las TIC hoy en día influencian las vías tradicionales de comercio y contratación. La World Wide Web y las medidas de contratación a través de aparatos electrónicos ya han introducido nuevas medidas de intercambio de bienes y servicios que se ofrecen en varios niveles en Internet[6].

A nivel global los gobiernos enfrentan el reto de impulsar y facilitar el desarrollo social y el crecimiento económico basado en las tecnologías emergentes de redes, y de proporcionar a sus ciudadanos una efectiva y transparente protección al consumidor en el comercio electrónico.

Existe una amplia variedad de leyes de protección al consumidor que regulan las actividades empresariales. Los países miembros de la OCDE[7] han iniciado, a finales de los años 90, la revisión de sus leyes vigentes así como de las prácticas de protección al consumidor, para determinar si se requiere o no realizar cambios en términos de las características particulares del comercio electrónico. Asimismo, los países miembros han estudiado la manera en que los esfuerzos de autorregulación pueden ayudar a proporcionar una protección efectiva y justa a los consumidores en este contexto.

En el momento actual, a nivel regional e internacional las posibilidades del comercio electrónico ya han sido analizadas y ampliamente utilizadas, existiendo mercados de bolsa, compañías aéreas, agentes y bancos que ofrecen la venta y la comercialización de bienes de todo tipo a través de la red.

Las firmas digitales[8] constituyen una herramienta esencial para garantizar la debida seguridad y brindar confiabilidad a las transacciones, facilitando y proporcionando autenticidad entre partes que no

---

6 Daniel Peña Valenzuela, *Lex Electrónica: ¿Mito o Realidad? Perspectiva desde la contratación por medios electrónicos* en *La Propiedad Inmaterial, Revista del Centro de Estudios de la Propiedad Intelectual de la Universidad Externado de Colombia*, Número. 7, página 103, 2003.

7 En abril de 1998, el Comité de Política del Consumidor de la OCDE inició el desarrollo de un conjunto de lineamientos generales para proteger a los consumidores en el comercio electrónico, sin crear barreras al comercio. Los Lineamientos constituyen una recomendación dirigida a los gobiernos, empresarios, consumidores y sus representantes, sobre las características esenciales que debe contener una efectiva protección al consumidor en el comercio electrónico. Este esfuerzo desembocó en un documento, "Recomendación del consejo de la OCDE relativo a los lineamientos para la protección al consumidor en el contexto del comercio electrónico" de 1999.

8 En términos generales, una firma digital es el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La tecnología para producir este resultado es lo que se conoce como cifrado asimétrico o cifrado de llave pública (Public Key Encryption).

necesariamente se han encontrado antes en el mercado, o que por varias razones nunca podrán hacerlo presencialmente. Por esta razón estas firmas constituyen un elemento imprescindible para el desarrollo del comercio electrónico o *e-commerce*.

Mientras que la firma digital hace referencia a una serie de métodos criptográficos, firma electrónica es un término de naturaleza fundamentalmente legal y más amplia desde un punto de vista técnico, ya que puede contemplar métodos no criptográficos[9].

En el *UNCITRAL model law on Electronic Commerce* adoptada en el 1996, las Naciones Unidas trataban de brindar seguridad al marco legal relativo al comercio electrónico, adaptando los requisitos legales ya entonces existentes, y aumentando el nivel de seguridad del proceso. Un aspecto importante fue la previsión relativa a la formación de la validez de un contrato electrónico. Con respeto a eso, este modelo de ley, establece que la información no se le puede negar el efecto legal o la validez o su aplicabilidad, solamente por el hecho de que la misma información sea presente en formato digital.

Con respeto a la normativa sobre comercio electrónico y contratación electrónica, actualmente varios países de la región han adoptado leyes que tratan de aplicar este *Model Law*: **Colombia** (1999), **República Dominicana** (2002), **Ecuador** (2002), **Guatemala** (2008), **México** (2000), **Panamá** (2001) y **Venezuela** (2001).

En la región, muchas de las legislaciones denominadas "leyes de comercio electrónico" abarcan más que esa temática. Además de incluir reglas sobre contratación electrónica, contienen normas sobre firmas electrónicas, certificados digitales y validez del documento electrónico.

En el *UNCITRAL Model Law on Electronic Signatures* adoptado en 2001, se aporta certidumbre jurídica a la firma electrónica. El modelo de ley, construida alrededor de la definición del artículo 7, establece una presunción: allí donde se alcanzan algunos criterios mínimos de compromiso técnico, la firma electrónica debe ser considerada igual a la firma original. La definición está conformada de forma tal que haya un enfoque técnico-neutral que no favorezca a ningún tipo particular de producto tecnológico.

Muchos países de la región como **Argentina** (2001), **Colombia** (1999) y **Ecuador** (2002) se han referido a este tipo de modelo.

Generalmente, mirando las varias normas de la región en esta materia (cuadro 1), se puede decir que:

- La casi totalidad (18/23) de los países de la región que han sido analizados cuentan con normativas específicas dedicadas a la materia de firma electrónica y firma digital.
- En los **23** casos analizados, **5** resultan no tener todavía una disciplina específica en la materia (**Bolivia, Cuba, El Salvador, Paraguay, Saint Lucia**), **4** resultan ser anteriores al 2000 (**Bermuda, Colombia, Puerto Rico, Uruguay**), mientras que **14** han sido realizadas en el período 2000-2009 (**Argentina, Barbados, Belize, Brasil, Chile, Costa Rica, Ecuador, Islas Caimán, México, Panamá, Perú, Trinidad y Tabago, Rep. Dominicana y Venezuela**). Lo que hace presumir que se trate de temáticas que recién han sido incluidas en normas o forman parte de reformas legislativas.

[9] Stephen Mason, Electronic Signatures in Law (Tottel, second edition, 2007).

CUADRO 1
REGIÓN DE AMÉRICA LATINA

Países	Firma electrónica y digital	Período de reforma	Observaciones
Argentina	**Ley Nº 25.506**. Firma electrónica: en caso de ser desconocida por su titular corresponde a quien la invoca acreditar su validez. **Decreto Nº 2628/02**, **Decreto N° 724/06**. Presunción "*iuris tantum*" de validez	2001	El Grupo Mercado Común (GMC) ha aprobado dos resoluciones que regulan sobre la eficacia jurídica del documento electrónico, la firma electrónica y firma electrónica avanzada y sobre los acuerdos de reconocimiento mutuo en el ámbito del MERCOSUR: MERCOSUR/GMC EXT./RES. Nº 34/06. El doc. aprueba las Directrices para la Celebración de Acuerdos de Reconocimiento Mutuo de firmas electrónicas avanzadas en el ámbito del MERCOSUR, donde se prevén algunas definiciones básicas, y se nombran los estándares internacionales de interoperabilidad que serán aplicados (www.mercosur.int/msweb/SM/Normas /Resoluciones/ES/2006/GMC_2006_RES_034_ES_Directrices.pdf) Los entes de previsión social de los países del Mercosur pondrán en funcionamiento a partir del 1° de julio la firma electrónica, para agilizar los trámites previsionales de los trabajadores de esos países, al reducir los tiempos en el intercambio de información.
Belize	**Capítulo 290:01**, Acta de Transacción Electrónica	2003	
Bermuda	Acta de **Transacción Electrónica,** 1999	1999	El acta refleja los estándares internacionales, incluyendo el UNCITRAL *Model Law* en comercio electrónico, estudios del Parlamento Europeo sobre firma electrónica, protección de información y legislación sobre "buenas prácticas" encontradas en otra jurisdicciones.
Bolivia (Estado Plurinacional de)	Ley de Documentos**, Firmas y Comercio Electrónico** de 2007	(2007)	Esta Ley se ha aprobado por unanimidad en el Congreso Boliviano en el mes de agosto de 2007, pero no se han encontrado referencias sobre su publicación en la Gaceta Oficial. **Todavía no tiene**
Brasil	**Medida provisoria 2.200-2** Que instituye el modelo de llave pública Brasileña (ICP)	2001	
Chile	**Ley 19.799** Firma electrónica, firma electrónica avanzada Disciplinado el uso de la F.E por parte de la Administración y los prestadores de los servicios de certificación (P.S.C.). art. 2 definición de documento electrónico	2002	F.E.A.: es aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría
Colombia	**Ley 527/1999** Del Comercio electrónico y de las firmas digitales.	1999	Cláusula de salvaguardia de los tratados internacionales vigentes - Definición amplia
Costa Rica	La **Ley 8454** de Firma digital, publicada el 13 de octubre de 2005. Sigue el **Reglamento 33018-MICIT** del 21 de abril de **2006**. No se hace referencia a la firma electrónica	2005/06	
Cuba	**Todavía no tiene**		
Ecuador	**Ley No. 2002-67** El Banco Central del Ecuador representa la primera Entidad de Certificación de Información y Servicios.	2002	La firma electrónica tiene igual validez que una firma manuscrita y que se le reconocen los mismos efectos jurídicos

(continúa)

Cuadro 1 (conclusión)

El Salvador	**Todavía no tiene**	2009	Se encuentra pendiente en el parlamento un anteproyecto de ley de comunicación y firma electrónica
Guatemala	Decreto **47-2008**, Ley para el reconocimiento de las comunicaciones y firma electrónica	2008	
Islas Caimán	The **Electronic Transactions Law**, 2000	2000	
México	**Decreto 29/5/2000** Reforma del código comercial para que la firma digital obtuviera valor jurídico. La ley atribuye valor jurídico a los certificados de gobierno y a las transacciones electrónicas/digitales	2000	Equivalencia funcional entre el consentimiento expresado por medios tecnológicos y la firma autógrafa "siempre que la información generada o comunicada en forma integra, a través de dichos medios sea atribuible a las personas obligadas y accesible para su ulterior consulta"
Paraguay	**Todavía no tiene**		Se están estudiando medidas para brindar validez jurídica a la firma electrónica y a los mensajes de datos, así como garantizar la eficacia probatoria de todo tipo de información en forma de mensaje de datos
Panamá	**Ley 43 del 31 de julio del 2001**	2001	La ley define y regula los documentos y firmas electrónicas, las entidades de certificación en el comercio electrónico, la prestación de servicios de certificación, el proceso voluntario de acreditación de prestadores de servicios de certificación y el intercambio de documentos electrónicos
Perú	**Ley 27269. Nuevo Reglamento** de la Ley de Firmas y Certificados Digitales aprobado por Decreto Supremo **052-2008**-PCM	2000	La Ley 27269 Otorga a la Firma Digital la misma validez que se le atribuye a la firma manuscrita. El reglamento reformula los contenidos y la regulación de los derechos digitales: derecho del ciudadano de acceso a servicios públicos electrónicos seguros; principios generales de acceso a los servicios públicos electrónicos seguros (legalidad; responsabilidad y calidad; presunción de reconocimiento y validez de los documentos electrónicos y medios de identificación y autenticación; seguridad, cooperación); derechos conexos
Puerto Rico	**S.B. 423 (188)** Digital Signature Acts	1998	
Saint Lucia	**Todavía no tiene**		Se encuentra pendiente un *draft* denominado: "**National Electronic Commerce Policy**" que prevé el estudio de una normativa sobre las firmas electrónicas
Trinidad y Tabago	The **Electronic Transactions** Bill, 2009	2009	Nuevo documento legal para dar fuerza legal a documentos electrónicos, grabaciones y firmas
Uruguay	**Decreto 65/998** de fecha 10 de marzo de 1998	1998	El decreto reglamentó el procedimiento administrativo electrónico. En su artículo 1 inciso final establece: "*Cuando la substanciación de las actuaciones administrativas se realice por medios informáticos, las firmas autógrafas que la misma requiera podrán sersustituidas por contraseñas o signos informáticos adecuados*". Los artículos 18-19 definen la firma electrónica y digital
Venezuela (República Bolivariana de)	**Decreto Ley N° 1204** dictado el **10/02/01**	2001	Otorga y reconoce eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, así como regula todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.

Fuente: elaboración propia con base en documentos presentes en los sitios Web de los Ministerios.

Ahora bien, al comparar las normas anteriores con aquellas de los países de la Unión Europea (cuadro 2), se ve claramente que América Latina, en cuanto al desarrollo de normas especificas en materia de firma electrónica, empezó un camino relativamente tardío. De hecho, de los **16** países analizados de la U.E., **6**

(Alemania, Austria, España, Italia, Luxemburgo, Portugal), tienen normativas específicas anteriores al año 2000, fecha que da indicios de los comienzos de regulación de la temática.

CUADRO 2
UNIÓN EUROPEA

Países	Acto legislativo	Año
Alemania	13 Junio 1997, Ley Alemana de Firma Digital	1997
Austria	Ley de Firma electrónica 1999	Aplicada desde el 2000
Bélgica	Ley de Firma electrónica	2001
Dinamarca	Ley número 417 del 31 de mayo de 2000	2000
España	Decreto-ley N° 14/1999 del 17 de septiembre de 1999	1999
Finlandia	Ley de Firma electrónica	2003
Francia	Decreto de firma electrónica del 31 de marzo de 2001	2001
Grecia	Decreto presidencial 150/2001	2001
Inglaterra	Acta de Comunicaciones Electrónicas	2000
Italia	D.P.R. 10 noviembre 1997 N° 513 (modificado por el decreto 445/2000)	1997
Irlanda	Acta Irlandesa de Comercio Electrónico, 2000	2000
Luxemburgo	Borrador de Ley 1998, modificado 1999	Aplicada desde el 2000
Noruega	Ley de Firma Electrónica	2001
Polonia	Acta de Firma Electrónica	2001
Portugal	Decreto-Ley Nº 290-D/99, del 2 de Agosto de 1999	1999
Rumania	Ley de Firma Electrónica, 455/2001	2001
Suecia	Ley de Firma Electrónica Calificada (SFS 2000:832)	2000

Fuente: elaboración propia.

Si bien con definiciones diferentes, el conjunto de normas analizadas tiende a:

1. otorgar y reconocer eficacia y valor jurídico a la firma electrónica, a mensajes de datos y a toda información inteligible en formato electrónico;
2. reconocer la eficacia probatoria de todo tipo de información en forma de mensaje de datos;
3. brindar validez a los documentos. Una vez creado un mecanismo para la certificación de la Firma, a la validez de la misma corresponderá la validez del documento electrónico entero;
4. introducir el concepto de Firma electrónica avanzada, como aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control.

La mayoría de los países presentan regulaciones basadas en infraestructura de claves públicas. Es decir que el usuario de un sistema genera un par de claves consistentes en una pública y otra privada, utilizando algoritmos asimétricos. Las claves tienen la característica que lo que cierra una, abre la otra y viceversa. La clave pública se distribuye a través de Autoridades Certificadoras que publican estás claves juntamente con los certificados de a quiénes pertenecen, mientras que la clave privada permanece secreta. Existen organismos gubernamentales o privados (pero bajo control de los gobiernos) de acreditación en Argentina (Secretaría de Gabinete y Gestión Pública), Brasil (Comité Gestor de Infraestructura de Llaves Públicas Brasileñas), Chile (Subsecretaría de Economía), Colombia (Sociedad Cameral de Certificación Digital, Certicámara, bajo la Superintendencia de Industria y Comercio), Ecuador (CONATEL), Panamá, Perú (Instituto Nacional de Defensa de la Competencia y de la Propiedad Intelectual), Puerto Rico, República Dominicana (Instituto Dominicano de Telecomunicaciones INDOTEL) y Venezuela.

Cuando se presenta este tipo de tecnología se tiende a pensar que hay implicaciones sólo para los técnicos y para aquellos que trabajan en informática por ejemplo, la verdad es que las firmas electrónicas tienen muchas implicaciones prácticas de uso cotidiano.

Como ejemplos, podemos mirar a los casos de **Brasil** y **Colombia**. En ambos países se pueden efectuar las declaraciones impositivas a través de Internet utilizando certificados digitales. La Secretaría de Hacienda Federal de Brasil permite que los contribuyentes posean su firma digital para presentar sus declaraciones y efectuar sus trámites ante el organismo en forma electrónica. Por su parte, la Dirección Nacional de Impuestos y Aduanas Nacionales de Colombia habilita el servicio de presentación de declaraciones impositivas electrónicas para los próximos vencimientos.

Otro ejemplo significativo es el caso de la emisión de facturas en forma electrónica[10], desarrollado por el Servicio de Impuestos Internos (SII) de **Chile**, hecho posible para empresas gracias a la Ley 19.799.

[10] http://www.e-certchile.cl/

III. Gobierno electrónico, acceso público a información y protección de datos

El manejo de la información almacenada por las administraciones públicas ha cambiado con el desarrollo de la tecnología de la información. La tecnología permite a los ciudadanos controlar el flujo de informaciones y datos en posesión de los gobiernos, generando implícitamente sobre éstos un mayor control.

El gobierno electrónico[11] consiste en el uso de las tecnologías de la información y el conocimiento en los procesos internos de gobierno y en la entrega de los productos y servicios del Estado tanto a los ciudadanos como al mercado.

El interés del sector público en el e-gobierno ha sido estimulado masivamente con el desarrollo del comercio electrónico entre los años 1995 y 2001[12]. En ese entonces, prácticamente todos los gobiernos del mundo desarrollado empezaban a tener en cuenta las TIC como un herramienta potente para mejorar la calidad de los servicios brindados a los ciudadanos.

En los países de América Latina el concepto de gobierno electrónico varía dependiendo de su implementación. La literatura[13] presenta la definición[14] de gobierno electrónico resaltando un listado de sus principales beneficios: (a) mejorar la calidad y el acceso a los servicios, (b) reducir costos administrativos, (c) restablecer la confianza de los ciudadanos, (d) evitar el desperdicio de recursos, (e) efectuar reingeniería de

---

[11] La *Gartner Group,* una de las principales empresa proveedora de servicios y asesora en tecnologías de la información, define e-gobierno como la "innovación continua de los servicios, la participación de los ciudadanos y la forma de gobernar mediante la transformación de las relaciones externas e internas a través de la tecnología, Internet y las nuevas formas de comunicación".

[12] Wimmer M., and Traumuller, R., Electronic Business invading the Public Sector: consideration on change and design, 34th Hawaii International Conference on System Sciences (HICSS), Hawaii 2001.

[13] La literatura sobre e-Gov es muy prolífica, y aquí no se pretende tomar en consideración todas las numerosas contribuciones relevantes, sino simplemente introducir la temática de manera general y ver cuales normativas de la región han innovado esta disciplina. De todas formas, cabe recordar algunas más significativas: Dunleavy, P., Margetts, H. "The Advent of Digital Government: Public bureaucracies and the state in the information age", Annual Conference of the American Political Science Association, Washington 2000; Chadwick, A. and May, C. "Interaction between States and Citizens in the Age of the Internet: 'e-Government' in the United States, Britain and the European Union, *Governance: An International Journal of Policy, Administration and Institutions* 16(2): 271-300, 2003; Peters, B.G. and Pierre, J. , Governance without Government? Rethinking Public Administration, Journal of Public Administration Research and Theory 8(2):223-243, 1998.

[14] Para un panorama de las múltiples definiciones, véase Moreno Escobar H., "Modelo multi-dimensional de medición del gobierno electrónico para América Latina y el Caribe, proyecto Sociedad de la Información", CEPAL, Naciones Unidas, Santiago 2007, Pág. 15.

procesos, (f) mejorar la infraestructura de tecnologías de información y comunicación, (g) entender la relación entre política y resultados, (h) decidir dónde gastar y cuándo, (i) rediseñar la entrega de servicios con calidad, transparencia y rendición de cuentas, (j) mejorar la capacidad de gobernar para atender los anhelos y expectativas de la sociedad, recuperando con ello la confianza en sus autoridades, (k) facilitar la implementación de la administración por objetivos, la creación de organizaciones más flexibles, el funcionamiento de estructuras menos piramidales y la creación de oficinas de gobierno más pequeñas y eficientes.

Dichos beneficios, por un lado han brindado servicios más eficientes y más rápidos a los ciudadanos, y por el otro han permitido un control más atento de los gobiernos. Las tecnologías ayudan a los ciudadanos a exigir más información y a controlar el uso que las administraciones públicas hacen de los datos sensibles que pertenecen a las personas.

Las Leyes de Transparencia y Acceso a la Información Pública han contribuido a regular los aspectos mencionados y a exigir una mayor rendición de cuentas (*accountability*), fomentando así la auditoría social. Un nivel mayor de transparencia garantiza a los pueblos un instrumento fuerte de evaluación de la gestión y el desempeño de los políticos elegidos. Hoy en día, sin duda, el tema de la transparencia de la administración pública, estrechamente relacionado con el gobierno electrónico, representa un asunto pendiente en la Región[15].

De acuerdo con la Organización para la Cooperación y Desarrollo Económico (OCDE), el gobierno electrónico se refiere al uso de las tecnologías de la información y comunicación, particularmente de Internet, como una herramienta para alcanzar un mejor gobierno (OCDE, 2004). En un informe de 2005 sobre el ejemplo **mexicano** de *e-government*[16], la OCDE analiza los lazos entre el gobierno electrónico y la necesidad de mayor transparencia. En términos de impacto de e-gobierno, el 73% de las agencias evaluada por parte del OCDE en México destacaban que había un importante efecto en la transparencia y *accountability* de la administración pública. Eso porque con la nueva Ley Mexicana de Transparencia[17], las agencias del Estado habían notado una mayor demanda de información por parte de los ciudadanos.

Son objetivos de la mencionada Ley (Art. 4 Ley Federal de Transparencia y Acceso a la información pública gubernamental):

1. proveer lo necesario para que toda persona pueda tener acceso a la información mediante procedimientos sencillos y expeditos;
2. transparentar la gestión pública mediante la difusión de la información que generan los sujetos obligados;
3. garantizar la protección de los datos personales en posesión de los sujetos obligados;
4. favorecer la rendición de cuentas a los ciudadanos, de manera que puedan valorar el desempeño de los sujetos obligados;
5. mejorar la organización, clasificación y manejo de los documentos, y
6. contribuir a la democratización de la sociedad mexicana y la plena vigencia del estado de derecho

El derecho de acceso a los actos, contratos y documentos en poder del Estado, es un tema relevante y esencial para las Sociedades del Siglo XXI, pero no debe ser confundido con la garantía del *"Habeas Data*[18]*"* (derecho al conocimiento, por parte de la persona, de sus propios datos) y con el principio de la

[15] Para un rápido resumen de las iniciativas de la Región, "E-ciudadanía, Practicas de buen Gobierno y TIC, Ester Kaufman, Documento preparado para la consulta regional del Programa Pan Américas IDRC 2005, Pág. 7.

[16] La encuesta se encuentra disponible en esta página Web: http://browse.oecdbookshop.org/oecd/pdfs/ browseit/4205161E.PDF.

[17] Ley federal de transparencia y acceso a la información pública gubernamental, de 11 de Junio de 2002.

[18] Se define como la acción constitucional o legal que tiene cualquier persona que figura en un registro o banco de datos, de acceder a tal registro para conocer qué información existe sobre su persona, y de solicitar la corrección de esa información si le causara algún perjuicio.

"*Autodeterminación Informativa*[19]" (derecho del interesado a ejercer control sobre informaciones que se refieren a si mismo) que amparan, desde fines de la década del 70, el derecho de cada persona para controlar y decidir exclusivamente sobre el procesamiento de sus datos personales y nominativos, sea por entes estatales o por empresas particulares.

La autodeterminación reviste un particular sentido hoy en día en el proceso penal, ya que a veces, para lograr los fines de la investigación de un hecho delictuoso se utilizan medios no admisibles o con violación a las reglas de la autodeterminación que también forman parte directa de las reglas del debido proceso. Un procesamiento de datos que no respete estos derechos, y utilice datos tanto sensibles como no sensibles para los efectos de la realización de perfiles de conducta para demostrar la participación criminal en un determinado hecho, debe ser considerado violatorio del debido proceso. Esto no significa que haya una carta blanca para que los delincuentes se rearmen con la herramienta informática o que estos queden fuera de la acción del Estado, sino que también en materia de derecho probatorio, y, sobre todo, cuando se trata de un procesamiento de datos con ese fin, se deben cumplir una serie de reglas y principios que forman parte integral del derecho procesal como derecho constitucional aplicado[20].

El derecho de acceso a la información pública de que se trata en este contexto, es una dimensión de la transparencia y consiste en la facultad que tiene toda persona de acceder a la información (que se refiera o no a ella misma) en poder de las instituciones públicas; es decir, es el derecho de solicitar y recibir la misma sin necesidad de acreditar que se tiene un interés legítimo ni de justificar la finalidad para la que se solicita la información.

Dando una mirada a la región, la materia del acceso a la información pública está regulada generalmente en leyes particulares, pero en las legislaciones de la Región se encuentra de manera dispersa y contradictoria, por ejemplo **El Salvador** cuenta con 126 leyes sobre información pública (fuente: Fundación salvadoreña para el desarrollo económico y social 2008).

De los 14 países analizados en la región (cuadro 3 - Argentina, Belize, Bolivia, Brasil, Chile, Colombia, Ecuador, Guatemala, Jamaica, México, Panamá, Perú, República Dominicana, Trinidad y Tabago) solamente dos tienen una normativa especifica en el tema, anterior al 2000 (**Colombia y Trinidad y Tabago**) lo que presenta este tipo de normas como relativamente reciente en América Latina y el Caribe. En algunos países recién comienzan a regir normas nuevas (**Chile, Guatemala**), o se están actualmente presentando proyectos de ley para colmar el vacío legislativo (como **Costa Rica** y **El Salvador**), lo que indica generalmente una tendencia hacia una mejor regulación de la materia.

En cuanto a **Brasil**, este país aún no ha establecido una ley especial para la libertad de la información. Sin embargo, el pasado 13 de mayo de 2009, la Presidencia de la República de Brasil envió un proyecto de ley de acceso a la información pública al Congreso Nacional[21].

El caso brasileño es peculiar ya que la ley tendrá alcance sobre todas las esferas del gobierno y en todos los niveles (federal, provincial y municipal). Se deberá definir instancias para recurrir o fiscalizar respetando la independencia de los municipios, Estados y el Distrito Federal; cada uno de estos niveles deberá crear sus propios organismos.

Con referencia al caso de **Chile**, ha sido recién aprobada la ley 20.285[22] sobre transparencia de la función pública y acceso a la información de los órganos de la Administración del Estado.

---

[19] Derecho fundamental derivado del derecho a la privacidad, que se concreta en la facultad de toda persona para ejercer control sobre la información personal que le concierne, contenida en registros públicos o privados, especialmente -pero no exclusivamente- los almacenados en medios informáticos.

[20] La discusión en el ámbito europeo, en especial en la República Federal de Alemania, donde el tema es altamente sensible, se ha desarrollado en la dirección de más cambios legislativos en el sentido de introducir límites al procesamiento de datos personales en manos de la policía y el ministerio público. Estos límites tienen como objetivo proteger a la persona de excesos que lesionen el principio de proporcionalidad y su derecho a la autodeterminación informativa. No se desea limitar las posibilidades de investigación o de comprometer el interés público en la obtención de la verdad real, sino que lo que se desea es que la calidad e intensidad del procesamiento de datos personales en este campo respete las reglas impuestas por la Sentencia sobre la Ley de Censos de 1983 del Tribunal Constitucional Federal Alemán, que es en este país la "carta magna" del procesamiento de datos.

[21] Fuente periodística: http://www.periodismo-aip.org/noticia-detalle.php?id=49

La norma legal, junto con crear un nuevo órgano llamado "Consejo de Transparencia", fue el resultado de una previa reforma constitucional, que contempló la incorporación de un nuevo artículo 8 dentro de las Bases de la Institucionalidad, que estableció que el ejercicio de las funciones públicas en Chile obligaba a sus titulares a dar estricto cumplimiento al principio de probidad en todas sus actuaciones, y se declaró perentoriamente que son públicos los actos y las resoluciones de los órganos del Estado, sus fundamentos y los procedimientos utilizados, pudiendo establecerse por excepción y sólo mediante una ley de Quórum Calificado su reserva o secreto. Este texto vino a fortalecer, para los ciudadanos, el llamado Derecho de Acceso a la Información relacionada con los actos y documentos de la Administración Estatal, antes también consagrado en el artículo 13 de la Ley de Bases de la Administración del Estado.

CUADRO 3
REFORMAS SOBRE GOBIERNO ELECTRÓNICO EN LA REGIÓN

Países	**Modernización de Admin. Pública/eGov.**	**Creación de algún órgano**	**Fuente**
Argentina	Decreto 378/2005, que establece el Plan Nacional de Gobierno Electrónico	Subsecretaría de gestión pública - Subsecretaría de Tecnologías de gestión. En su primera Resolución (Res. 01/2008), se creó el Programa Directorio del Poder Ejecutivo Nacional, en el marco del Plan Nacional de Gobierno Electrónico. El Decreto 378/2005 dicta los lineamientos estratégicos que han de regir el Plan Nacional de Gobierno Electrónico y los Planes Sectoriales de los organismos de la Administración Pública Nacional (APN)	www.sgp.gov.ar/contenidos/onti/productos/pnge/pnge.html
Bolivia (Estado Plurina-cional de)	Decreto Supremo N° 26553 de fecha 19 de marzo de 2002: las Tecnologías de Información y Comunicación (TIC) son herramientas útiles para lograr las metas de desarrollo de forma más eficiente. Decreto Supremo 26624, reglamenta y ordena el registro de nombres de dominio en Internet en el país (14 de mayo 2002);	ADSIB Agencia para el desarrollo de la Sociedad de la Información en Bolivia	www.adsib.gob.bo
Brasil	No hay un texto legal específico.	Secretaría de Logística y Tecnología de la Información - SLTI. Planea, ordena, gestiona y es responsable de reglamentar compras y contrataciones y también para normas relacionadas al uso de Tecnología de la Información en el ámbito de la Administración Pública Federal. Los trabajos de SLTI tienen como objetivo ampliar la transparencia y el control social sobre las acciones del Gobierno Federal.	http://www.planejamento.gov.br/secretaria.asp?sec=7

(continúa)

[22] La Ley fue aprobada para elevar los estándares de Chile en material de protección de datos personales como pedido por parte de la OCDE.

Cuadro 3 (continuación)

Chile	Ley 20.285 sobre transparencia de la función pública y acceso a la información de los órganos de la Administración del Estado. Creación del "Consejo de Transparencia. Disciplinado el Derecho de Acceso a la Información, relacionada con los actos y documentos de la Administración Estatal, antes también consagrado en el artículo 13 de la Ley de Bases de la Administración del Estado.	Consejo de Transparencia (registro obligatorio de responsables de bases de datos personales)	www.habeasdataorg.cl
Colombia	Ley n. 962 de 2005, por la cual se "dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos" (ley anti-trámites). El documento CONPES 3072 de 2000 consagra la Agenda de Conectividad como política de Estado. Teniendo en cuenta el Marco Regulatorio que se tiene actualmente en el Documento Visión 2019, el Plan de Gobierno de la actual administración de Gobierno y las normas, leyes y decretos que rigen al sector, al igual que las regulaciones de la Comisión de Regulación de Telecomunicaciones CRT, hasta el momento se cuenta con: - El Decreto 2870 del 31 de julio de 2007, el cual busca facilitar la entrada de nuevos inversionistas y optimizar la utilización de la infraestructura de telecomunicaciones existente con el fin de desarrollar servicios apoyados en las TIC. - El Proyecto de Ley Cámara 112 de 2007, radicado en septiembre del mismo año, por el cual se crea la Agencia Nacional de Espectro. - En Agosto de 2007 la CRT expidió el régimen de protección a los usuarios de telecomunicaciones, el cual garantiza la adecuada protección de dichos usuarios en un entorno de convergencia. Así mismo, se expidió en octubre del mismo año la Resolución 1740, en la cual se fijan parámetros para la calidad de los servicios de telecomunicaciones.	Agenda de conectividad. El Programa Agenda de Conectividad, del Ministerio de Comunicaciones de Colombia, es el responsable de impulsar el desarrollo de la Estrategia de Gobierno En Línea	www.mincomunicaciones.gov.co
Costa Rica	Reforma Integral del Decreto Ejecutivo Nº 33147-MP que crea la Comisión Intersectorial de Gobierno Digital y la Secretaría Técnica de Gobierno Digital. Presidida por el Segundo Vicepresidente de la República e integrada por varios otros Ministros.	Secretaria Técnica de Gobierno Digital de la Presidencia de la República y Comisión Intersectorial de gobierno digital	www.gobiernofacil.go.cr/gobiernodigital/index.html

(Continúa)

Cuadro 3 (continuación)

Ecuador	CONATEL, Programa nacional para el gobierno electrónico y la sociedad de la información. En el documento se hace referencia a la situación del gobierno electrónico: a) inexistencia de estandarización en la presentación de los pocos portales del gobierno; b) Ineficiencia en el gasto de acceso a Internet y arrendamiento de circuitos en las entidades del sector público	Comisión Nacional de Conectividad, Comisión técnica Especial de gobierno en Línea	www.conatel.gov.ec; www.imaginar.org/index_archivos/gobierno/ecuador.pdf
El Salvador	No hay un texto legal específico.	Secretaría Técnica de la Presidencia	www.servicios.gob.sv
Guatemala	Acuerdo gobernativo n. 364/2004 de 4 nov. 2004	Comisión presidencial para la reforma, modernización del Estado, subordinada a la Presidencia de la República	
México	Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público	Unidad de gobierno electrónico y Política de Tecnologías de la Información (UGEPTI) de la Secretaria de la Función Pública y Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico. Creada en 2001	http://www.gobierno-digital.gob.mx/wb/gobDigital/gobD_GobiernoElectronico; http://www.e-mexico.gob.mx/
Paraguay	Decreto 7070/2006 prevé que cada Agencia gubernamental debe entregar cada mes un informe de gastos públicos, actividades realizadas, empleados y salarios a la Secretaria Nacional Pública para que los datos sean públicos y accesibles	Secretaria Técnica de Planificación de la Presidencia de la República	http://www.stp.gov.py/
Panamá	Decreto Ejecutivo n. 102/2004	Secretaria de la Presidencia para la Innovación Gubernamental	http://www.innovacion.gob.pa/
Perú	Decreto Supremo 94/2005	ONGEI Oficina Nacional de Gobierno Electrónico e Informática	http://www.ongei.gob.pe/
Uruguay	Ley n. 17.930	Agencia para el Desarrollo del Gobierno Electrónico y de la Sociedad de la Información y del Conocimiento	http://www.agesic.gub.uy/Sitio/
Venezuela (República Bolivariana de)	Decreto n. 737/2000	Centro Nacional de Tecnologías de la Información (CNTI)	http://www.cnti.gob.ve/

Fuente: elaboración propia.

IV. Delitos informáticos y cibercrimen

Para introducir este complejo tema cabe citar a Manuel Castells. En ocasión de un discurso del 2001[23], y hablando del "caos" positivo que Internet genera en la comunicación, Castells dijo: "Técnicamente, Internet es una arquitectura de libertad. Socialmente, sus usuarios pueden ser reprimidos y vigilados mediante Internet. Pero, para ello, los censores tienen que identificar a los trasgresores, lo cual implica la definición de la trasgresión y la existencia de técnicas de vigilancia eficaces. La definición de la trasgresión depende, naturalmente, de los sistemas legales y políticos de cada jurisdicción. Y aquí empiezan los problemas. Lo que es subversivo en Singapur no necesariamente lo es en España". En seguida citó el ejemplo de cuando en 2000 un sitio Web de EE.UU. organizó la venta de votos de personas ausentes, hecho que representaba un delito electoral en ese país. Pero la Web se mudó a Alemania, donde ese hecho ya no podía ser perseguido por las leyes de ese país.

Esta introducción aclara el lado débil de esta materia. La red expone los usuarios a conductas que no necesariamente pueden ser automáticamente sancionadas en el lugar donde se accede a la Web. Eso porque las leyes penales de los países son diferentes y en épocas donde las personas se movían menos, y las comunicaciones no eran tan frecuentes y tan tecnológicamente avanzadas, no surgía muy a menudo la preocupación de crear normas penales de aplicación transnacional. Los crimines cibernéticos característicamente se originan en jurisdicciones que tienen legislación débil o inexistente acerca de este tema. Un ataque de tipo viral que costó a empresas norteamericanas miles de millones de dólares fue atribuido por el FBI a un estudiante en Filipinas, donde no se le pudo acusar de crimen alguno. Rápidamente el gobierno filipino implantó legislación para combatir el crimen cibernético, y muchos países han intentado lo mismo[24]. Sin embargo, existen todavía vacíos legales que los criminales aprovechan.

Los crímenes cometidos a través de las TIC[25] (el crimen está sancionado y se perfecciona exista o no la presencia de TIC – ejemplo: ciberterrorismo, si no hay medios tecnológicos solo habrá el delito de terrorismo) y en las TIC (el delito no se perfecciona si no hay presencia/uso de TIC – ejemplo: *phishing*, o sea una estafa que se realice a través de Internet), se caracterizan todos por un altísimo nivel de transnacionalidad: las estructuras de estos crímenes incluyen normalmente más de un país (el país donde la acción criminal ha sido pensada, el país donde la acción criminal viene tramitada y finalmente el país donde se realice el daño a la persona que el derecho penal

[23] "Internet, libertad y sociedad: una perspectiva analítica", Conferencia inaugural del curso académico 2001-2002 de la UOC.

[24] Phil Williams, "Organized Crime and Cybercrime: Synergies, Trends, and Responses", International Information Programs, Electronic Journal of the U.S. Department of State – August 2001 Volume 6, Number 2

[25] Para una sistematización del derecho penal de la informática véase: Téllez Valdés, Julio, "Derecho Informático", 3ª ed., Ed. Mac Graw Hill, México,

sanciona). Se puede decir que la delincuencia informática, como conjunto de los varios crímenes que se denotan por la presencia de alguna tecnología, es un fenómeno global, como es global la red, y por lo tanto, si se quiere limitarlo, la coordinación a nivel internacional es una necesidad imprescindible. De hecho, a pesar de que existe un creciente movimiento para crear marcos legales comunes, o simplemente principios de Derecho Penal Internacional[26], todavía no se ha llegado a desarrollar un concepto internacional de delitos informáticos, por lo que sigue siendo un fenómeno estudiado a nivel prevalentemente nacional.

En cuanto a los términos utilizados para definir la problemática, en la literatura en lengua española se ha ido imponiendo la expresión de delito informático, que, según el Profesor Casabona[27]*: "…tiene la ventaja de su plasticidad, al relacionarlo directamente con la tecnología sobre o a través de la que actúa. Sin embargo en puridad no puede hablarse de un delito informático, sino de una pluralidad de ellos, en los que encontramos como única nota común su vinculación de alguna manera con los computadores, pero ni el bien jurídico protegido agredido es siempre de la misma naturaleza ni la forma de comisión del hecho delictivo -o merecedor de serlo- presenta siempre características semejantes... el computador es en ocasiones el medio o el instrumento de la comisión del hecho, pero en otras es el objeto de la agresión en sus diversos componentes (el aparato, el programa, los datos almacenados). Por eso es preferible hablar de delincuencia informática o delincuencia vinculada al computador o a las tecnologías de la información*."

La delincuencia informática se puede definir en un sentido amplio, como todo delito que implique la utilización de las tecnologías informáticas.

Las nociones de «delincuencia informática», «delincuencia relacionada con la informática», «delincuencia de alta tecnología» y de «delincuencia cibernética» tienen el mismo significado en cuanto se refieran a: a) la explotación de las redes de información y comunicación sin ninguna dificultad geográfica y b) la circulación de datos intangibles y volátiles.

En suma, los principales delitos tratados por la legislación existente a nivel internacional son los siguientes:

1. delitos contra la propiedad intelectual: delitos contra la protección jurídica de programas de ordenador y la protección jurídica de las bases de datos, los derechos de autor y derechos afines;
2. delitos contra la intimidad: recogida, almacenamiento, modificación, revelación o difusión ilegales de datos personales;
3. delitos relativos al contenido: difusión, especialmente por Internet, de pornografía, y en especial de pornografía infantil, declaraciones racistas e información que incita a la violencia;
4. delitos económicos, acceso no autorizado y sabotaje: muchos países han aprobado leyes que abordan los delitos económicos perpetrados por ordenador y tipifican nuevos delitos relacionados con el acceso no autorizado a sistemas informáticos (por ejemplo, la piratería, el sabotaje informático, la distribución de virus, el espionaje informático, la falsificación y el fraude informáticos).

Sin embargo, se ha visto que la estrategia de modificación normativa no es suficiente, y en algunos casos, como en la Unión Europea, se empezaron a implementar algunas medidas no legislativas. Entre ellas cabe recordar la creación de unidades nacionales especializadas (autoridades policiales y autoridades judiciales); la formación permanente y especializada de policías y personal de la administración de justicia; la armonización de las normas de contabilización en materia policial y judicial así como la creación de instrumentos adaptados para el análisis estadístico de la criminalidad informática; creación de acciones realizadas directamente por las empresas con el fin de luchar contra la delincuencia informática; implementación de proyectos en el ámbito de la investigación y el desarrollo tecnológico (IDT).

Las medidas no legislativas mencionadas encuentran un límite fundamental en los recursos. El tema de los recursos afecta generalmente la capacidad de frenar la propagación de estas formas criminales, ya que en los pocos países en los que hay unidades de policía especializadas en estos delitos los funcionarios no cuentan ni con

[26] Véase: Sunga, Lyal S. *The emerging system of international criminal law: developments in codification and implementation*, The Hague, Kluwer Law International 1997.

[27] Romeo Casabona, Carlos María**,** Poder Informático y Seguridad Jurídica, Fundesco, Madrid, España, 1987.

la tecnología ni con la capacitación requeridos. Según fuentes periodísticas (El Clarín) el Centro de Investigación en Seguridad Informática (CISI) de Argentina, realizó un estudio que estima en que el 43% de las empresas que en 2005 reconoció haber tenido algún "incidente" en sus sistemas, lo que llevó a que el 63% de las consultadas señalara que preveía una mayor inversión en la seguridad de sus sistemas de computación y almacenamiento de datos[28]. Este dato se refería solamente a las entidades privadas, pero indica claramente que sin recursos es muy difícil oponerse a estos tipos de crímenes, aun en presencia de normas especificas.

Durante los últimos diez años el avance normativo a nivel regional ha estado focalizado en la penalización del uso de las TIC sobre todo en temáticas más sensibles, como el caso de la pornografía infantil, y en el desarrollo del peritaje forense y la creación de "brigadas digitales" o cuerpos especializados para lucha contra estos tipos de crímenes.

En **Perú,** existe la Dirección de Investigación Criminal y de Apoyo a la Justicia, con su División de Delitos de Alta Tecnología; que es parte de la Policía Nacional del Perú (PNP). Cuentan con tres departamentos: i) Departamento de Delitos Informáticos, Patrullaje Virtual, ii) Departamento de Investigación Especial (Hurto de Fondos, Pornografía Infantil, Piratería de Software, Investigaciones Especiales) y iii) Departamento de Coordinación, Coordinación Búsqueda de Información.

En **Bolivia,** existe la División Delitos Informáticos que es parte de la Fuerza Especial de Lucha Contra el Crimen FELCC de la Policía Nacional.

En **Colombia,** existe el grupo de delitos informáticos de la SIJIN (Policía Nacional) quien tiene varios laboratorios de computación forense, y el DAS (Departamento Administrativo de Seguridad) que tiene una unidad específica de delitos informáticos, además de varias entidades investigativas privadas que colaboran con los agentes nacionales (antifraude.org).

En **Uruguay,** está presente la sección Delitos Informáticos del Departamento de Delitos Complejos, de la Dirección de Investigaciones de la Jefatura de Policía.

En **Ecuador,** existe la DIDAT, Departamento de Investigación de Alta Tecnología de la Policía Judicial del Ecuador, además en la Fiscalía General del Estado existe el Departamento de Investigación y Análisis Forense.

En **México,** la Policía Cibernética de la Secretaría de Seguridad Pública Federal, trabaja en temas de delitos informáticos, llevando a cabo campañas de prevención del delito informático a través de la radio y cursos en instituciones públicas y privadas. También está el equipo UNAM-CERT que, sin tener la misión de perseguir los delitos cibernéticos, igual realiza acciones contra sitios de *phishing* y análisis forense.

En **Chile**, desde el año 2000, existe la "Brigada Investigadora del Ciber Crimen", dependiente de la Jefatura Nacional de Delitos Económicos. Esta Brigada se compone de tres entidades principales: el Grupo de Investigación de Pornografía Infantil, el de Delitos Financieros e Investigaciones Especiales y el de Análisis Forense Informático.

En América Latina se considera que no existe una cantidad suficiente de leyes en materia de delitos informáticos para las diferentes tipologías de crímenes. Se nota una gran diversidad de delitos y al mismo tiempo una gran cantidad de bienes jurídicos que estas normas quieren proteger. Hay casos de delitos contra el patrimonio, delitos contra la propiedad (física o intelectual), delitos contra las personas (contra la Intimidad, el derecho a la propia imagen y la inviolabilidad de domicilio), delitos contra la hacienda pública nacional que han sido tratados por normativas diferentes, a veces con reformas de los códigos penales, a veces con leyes *ad hoc*, en última instancia hasta con leyes de comercio electrónico.

En la Región (cuadro 4) el intento de regular estos fenómenos criminales ha encontrado diferentes soluciones a nivel legislativo. Aparentemente, la mayoría de los países analizados ha preferido reformar sus

[28] Fuente: diario "Clarín", ejemplar del 27 de junio de 2005, Pág. 29, nota titulada "Temor por el robo de datos en Internet", citado por Marcelo A. Riquert, Algo más sobre la Legislación contra la Delincuencia Informática en MERCOSUR a propósito de la Modificación al Código Penal Argentino por Ley 26388.

códigos penales (**Argentina, Bolivia, Costa Rica, Guatemala, México, Paraguay, Perú**), mientras que algunos han introducido leyes específicas en la materia (**Brasil, Chile, Colombia, Venezuela**). **Ecuador** ha utilizado una ley de contenido civil-comercial como la de comercio electrónico para introducir normas penales, y **Uruguay** solamente prevé una ley de Protección del Derecho de Autor. Cabe señalar que en los países donde no ha habido todavía habido una reforma en este campo, se trata de "reinterpretar" la normativa vigente en materia penal para incluir tipologías de delitos informáticos que no son reguladas por normas particulares (Ej. Uruguay donde se aplican las disciplinas clásicas de los delitos de hurto, estafa o daño a casos donde estos delitos han sido cometidos con uso de tecnología). Bajo un punto de vista legal, este proceso de adaptación de la normativa general a casos particulares, no previstos, aumenta el riesgo de impunidad, porque algunos delitos informáticos pueden no tener los requisitos mínimos de parecidos hechos penales "clásicos" (el delito de hurto en muchas legislaciones necesita de la presencia de una "posesión física" por parte del sujeto que roba, cosa que no pasa si un estafador online simplemente usa los datos de otra persona sin que los mismos entren "físicamente" en su posesión). Al no estar tipificado el delito informático se debería acudir al principio de legalidad en materia penal "*nullum crimen nulla poena sine lege*".

CUADRO 4
REFORMAS EN MATERIA DE DELITOS INFORMÁTICOS

Países	Acto normativo	Contenido	Técnica
Argentina	Ley 26388 26/6/08 reforma del código penal argentino	Contenido: Pornografía infantil por Internet u otros medios electrónicos (Art. 128 CP); • Violación, apoderamiento y desvío de comunicación electrónica (Art. 153, párrafo 1º CP); • Intercepción o captación de comunicaciones electrónicas o telecomunicaciones (Art. 153, párrafo ºCP); • Acceso a un sistema o dato informático (artículo 153 bis CP); • Publicación de una comunicación electrónica (artículo 155 CP); • Acceso a un banco de datos personales (artículo 157 bis, párrafo 1º CP); • Revelación de información registrada en un banco de datos personales (artículo 157 bis, párrafo 2º CP); • Inserción de datos falsos en un archivo de datos personales (artículo 157 bis, párrafo 2º CP; anteriormente regulado en el artículo 117 bis, párrafo 1º, incorporado por la Ley de Hábeas Data); • Fraude informático (artículo 173, inciso 16 CP); • Daño o sabotaje informático (artículos 183 y 184, incisos 5º y 6º CP)	Reforma código penal (La Ley 26.388 no es una ley especial, que regula este tipo de delitos en un cuerpo normativo separado del Código Penal (CP) con figuras propias y específicas, sino una ley que modifica, sustituye e incorpora figuras típicas a diversos artículos del CP actualmente en vigencia)
Bolivia (Estado Plurinacional de)	Código Penal Boliviano, texto ordenado según ley No 1768 de 1997, incorpora en el Título X un capítulo destinado a los Delitos Informáticos.	La Ley No 1768, no obstante de no estar exenta de la problemática actual, al abordar en el Capítulo XI la tipificación y penalización de delitos informáticos, no contempla la descripción de estas conductas delictivas detalladas anteriormente. Por consiguiente, la atipicidad de las mismas en el ordenamiento jurídico penal boliviano vigente imposibilita una calificación jurídico-legal que individualice a la mismas, llegando a existir una alta cifra de criminalidad e impunidad, haciéndose imposible sancionar como delitos, hechos no descriptos en la legislación penal con motivo de una extensión extralegal del ilícito penal ya que se estaría violando el principio de legalidad expreso en la máxima "*Nullum crimen sine lege*".	Reforma código penal
Brasil	Ley 8137 (27/12/90), sobre "Crímenes contra el orden económico y las relaciones de consumo"	Uso ilícito del ordenador, que sería la acción de utilizar o divulgar programas de procesamiento de datos que permita al contribuyente poseer información contable diversa que es, por ley, proporcionada a la Hacienda Pública.	Ley especial

(continúa)

Cuadro 4 (continuación)

	Ley 7646/1987	Violación de derechos de autor de programas de ordenador	Ley especial
	Ley 9100, Art. 67 inc. VII.	Acceso a bancos de datos. Tipo penal para punir con reclusión de uno a dos años y multa la obtención indebida de acceso, o su intento, a un sistema de tratamiento automatizado de datos utilizado por el servicio electoral, con el fin de alterar el cómputo o cálculo de votos	Ley especial
Chile	Ley 19.223/1993 sobre delitos informáticos	Figuras previstas: 1.- acceso indebido a información contenida en un sistema de tratamiento de la misma; 2.- destrucción de un sistema informático o alteración del funcionamiento del mismo; 3.- daño, alteración y divulgación indebida de datos informáticos. Nuevo proyecto de ley (mensaje del Ejecutivo boletín Nº 3083-07) que introduce nuevos delitos informáticos, no especialmente incriminados en la legislación anterior; a saber: 1.- falsificación de documentos electrónicos y tarjetas de crédito 2.- fraude informático; y 3.- obtención indebida de servicios de telecomunicaciones.	Ley especial
Colombia	Ley 679 de 2001 sobre pornografía infantil en redes globales	Medidas de protección contra la explotación, la pornografía, el turismo sexual y demás formas de abuso sexual con menores de edad, mediante el establecimiento de normas de carácter preventivo y sancionatorio	Ley especial (El Código Penal Colombiano expedido con la Ley 599 de 2000, no hace referencia expresa a los delitos informáticos como tales)
Costa Rica	Ley No. 8148	Adición de los artículos 196 bis, 217 bis y 229 bis al Código penal; ley n. 4573 para reprimir y sancionar los delitos informáticos. Figuras: Violación de comunicaciones electrónicas, Fraude informático, Alteración de datos y sabotaje informático,	Código penal
Cuba	Reglamento de Seguridad Informática en vigor desde Noviembre de 1996	Estipula que en todos los Órganos y Organismos de la Administración Central del Estado se deberán analizar, confeccionar y aplicar el "Plan de Seguridad Informática y de Contingencia"; y el Reglamento sobre la protección y seguridad técnica de los sistemas informáticos, emitido por el Ministerio de la Industria Sideromecánica y la Electrónica, también en vigor desde Noviembre de 1996.	Reglamento
Ecuador	Ley No. 2002-67, de comercio electrónico, firmas y mensajes de datos. Ningún instrumento legal específico. Referencia a la tipificación del código		Algunas normas penales en la ley de comercio electrónico.
El Salvador	Código penal. No consta disciplina específica		Código penal
Guatemala	Código penal - CAP VII (De los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos) Código del 1973, reformado en este capítulo en 1996 y 2000.	Figuras: tutela derecho de autores (robo uso y gestión de obras sin la autorización del autor); destrucción de registros informáticos; manipulación de información; violación a los derechos de propiedad industrial	Código penal

(continúa)

Cuadro 4 (conclusión)

México	El código penal mexicano fue reformado con Ley el 17 mayo 1999. El título Décimo del Código Penal, en la sección sobre "Delitos contra el patrimonio", prevé en el artículo 217 del referido texto legal al delito informático.	Comete delito informático: "la persona que dolosamente y sin derecho intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red, se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días de multa". El código no contempla todos los tipos más comunes de ataques informáticos. El capítulo II (como reformado en 1999) se refiere a los "accesos ilícitos", poniendo de hecho un límite a su aplicación, ya que no todos los ataques informáticos se perpetran necesariamente con acceso directo a un sistema. Ejemplo es el caso de "*denial of service*" que, según el código penal federal, tiene como objetivo el de modificar, destruir o provocar la pérdida de información. La conducta de aquel que simplemente imposibilita o inhabilita temporalmente un servidor no vendría entonces a caer en el marco de la norma citada.	Código penal
Paraguay	Art. 184 del C.P. (1997), en función de la Ley 1328/1998 "De Derecho de Autor y Derechos Conexos	Violación del derecho de autor o inventor	Reforma código penal
Perú	ley 26612/1996	Espionaje industrial	
	ley 27309, ley de incorporación de los delitos informáticos al código penal	Figuras: ingreso o interferencia en bases de datos, sistema o red de computadores.	Ley especial de incorporación de los delitos informáticos en el código penal
	Proyecto de ley No. 2825-2000/CR, sobre pornografía infantil en Internet	El proyecto trata de tipificar e incorporar en el Código Penal el tipo penal de pornografía infantil que contemple tanto la conducta de procurar y facilitar que los menores de dieciocho años realicen actos de exhibicionismo corporal, lascivos y sexuales con el objeto y fin de fotografiarlos o exhibirlos mediante anuncios impresos o electrónicos, con o sin el fin de obtener un lucro, como la de fijar, grabar, imprimir, actos de exhibicionismo corporal lascivos y sexuales con menores de dieciocho años y la de elaborar, reproducir, vender, arrendar, exponer, publicitar o trasmitir el material pornográfico.	
Uruguay	Ley de Protección del Derecho de Autor y Derechos Conexos Nº 17.616 (13 de enero de 2003)	Normas que tutelan solamente la propiedad intelectual (software)	Ley especial (se trata de buscar un aplicación amplia de las figuras clásicas introducidas por el código penal: hurto, estafa, daño)
Venezuela (República Bolivariana de)	Decreto 48/2001(Ley Especial Contra los Delitos Informáticos)	Hasta entonces se extendían las tipologías penales del código penal de 1964.nuevas figuras contempladas: sabotaje, daño de sistemas, falsificación documentos, acceso indebido, espionaje informático, violación de privacidad o de datos personales, relevación indebida de información personal, difusión o exhibición de material pornográfico adulto o de niños/adolescentes, apropiación de propiedad intelectual	Ley especial

Fuente: elaboración propia, algunos datos del grupo en derecho informático de alfa-redi, http://dgroups.org/Community.aspx?c=423d0743-7537-4277-bef7-351b42c853e1

La Convención sobre el cibercrimen

El objetivo de esta convención internacional es recurrir a la colaboración internacional entre países, de manera de se establezca que una conducta lesiva sea delito en cada jurisdicción. Así, no obstante se mantengan y se respeten las legislaciones locales, los Estados deben definir delitos informáticos basados en un modelo común. La Convención sobre cibercrimen, firmada en Budapest en 2001, entró en vigencia el 1º de julio de 2004 y en su redacción participaron los 41 países miembros del Consejo de Europa, junto a otros Estados no miembros como Estados Unidos, Canadá, Japón y Sudáfrica. La convención no se encuentra actualmente vigente en ningún país de América Latina y el Caribe.

El enfoque subyacente de la Convención es reconocer la necesidad de armonizar las legislaciones nacionales. La Convención introduce elementos de derecho sustancial penal, junto a previsiones de derecho procesal, principios para la coordinación internacional, extradición, medidas provisionales. En otras palabras, trata del argumento en manera completa y exhaustiva, dictando normas y sugiriendo reglas de organización entre diferentes instituciones policiales.

En el sector penal, la armonización se ha logrado en materia de tratados de extradición y de existencia legal mutua que permite a los gobiernos compartir información y evidencia. Existe por ejemplo el requerimiento de la llamada dualidad criminal (el acto que se investiga debe ser un crimen en ambas legislaciones; los gobiernos deben tener la capacidad de aplicar las leyes).

Los delitos cibernéticos frecuentemente tienen implicaciones de seguridad nacional y de procedimientos de inteligencia, lo cual complica la colaboración. Por lo tanto, resultará útil establecer redes de confianza entre las agencias encargadas de combatir el crimen cibernético en los diversos países para crear una red de investigación y punición que no sea obstaculizada con las fronteras.

V. Los sistemas judiciales y las TIC. Algunas buenas prácticas en la región: Uruguay, Perú, Brasil y Chile

La justicia en el nuevo paradigma tecnológico ha creado su propio espacio y desafíos. A pesar de que tradicionalmente la inversión tecnológica en este campo no ha ido al mismo ritmo que en otros (comunicación, comercio), esta tendencia ha ido cambiando en la última década, demostrado por las iniciativas de muchos gobiernos en materia de innovación en los sistemas judiciales.

Tal como afirma Fernando Jordán, en su libro Las Nuevas Tecnologías, el Derecho y la Justicia "La función del Derecho consiste en adecuarse a las nuevas necesidades de la sociedad, para establecer continuamente, las nuevas reglas de convivencia, los procedimientos y los sistemas de control y coerción, de organización y de convivencia, en un mundo globalizado y cambiante"[29].

Ahora bien, hay que delimitar el sentido del concepto de e-justicia, o aplicación de las TIC a la administración de la Justicia. Al hablar de la administración de justicia o de "justicia" en términos generales, se hará referencia principalmente a la resolución de conflictos entre partes o a la asignación de derechos de distinta naturaleza realizada por tribunales de justicia. Dentro de éstos, están los delitos penales, las reclamaciones civiles, los conflictos de familia, los conflictos en las relaciones laborales, las reclamaciones administrativas de la actuación del Estado, entre varios aspectos contemplados en las leyes de cada país.

Cabe recordar que la administración de justicia en América Latina ha sido vista con altos niveles de desconfianza por la ciudadanía[30]. Sin pretender hacer un análisis exhaustivo, en la generalidad de los países de la Región, el modelo tradicional de impartición de justicia es señalado usualmente como lento, excesivamente formalista y burocrático, y lejano para el común de la ciudadanía. Estas percepciones pueden tener su origen en dos elementos particulares de la forma en que tradicionalmente se ha administrado justicia en la Región, que son la escrituración formalista de los procesos judiciales y la especial organización de estas instituciones, las que traen como consecuencia una inadecuada organización en el despacho judicial, que es donde finalmente se tramitan los casos.

En todo caso, pese a un general sentido de desconfianza en estas instituciones, mucho se está desarrollando para que las TIC brinden mayor eficacia a la administración de la Justicia.

---

[29] Jordán Florez, Fernando, Las Nuevas Tecnologías, el Derecho y la Justicia, Servigraphic, LTDA, Colombia, 2000. Página 21.

[30] El porcentaje de personas en América Latina que en el 2007 dijo tener "algo" o "mucha" confianza en el gobierno fue de 39%. Respecto al Poder Judicial, esa misma medición indicaba el 30%. Ver http://www.latinobarometro.org/. Para ver indicadores relacionados con la gobernabilidad y control de la corrupción de nivel mundial, ver http://siteresources.worldbank.org/INTWBIGOVA NTCOR/Resources/wps4370.pdf

Un estudio realizado por el Centro de Estudios de Justicia de las Américas, (CEJA), sobre el foro **"**El uso de información en las instituciones de justicia", plantea que: "El enorme salto tecnológico que se ha dado en los últimos años en el manejo y uso de los sistemas de información ha impactado de un modo inocultable los viejos modelos y ha generado nuevas expectativas sobre la base de la información que debe tener una decisión para ser considerada como razonable y justificada. Es decir, que nos hallamos ante una organización necesariamente en transición donde el uso de la información deberá *cumplir una triple función:* por una parte, debe ayudar a esa transición, asumiendo que los procesos de toma de decisión todavía no están *normalizados* y por lo tanto serán una mezcla de nuevas y viejas formas. Pero de todos modos el sistema judicial debe seguir funcionando y debe transformase sobre la marcha. En segundo lugar, los sistemas de información deben acompañar y *ayudar a moldear* los nuevos procesos de toma de decisión que surjan de los nuevos modelos organizacionales. En tercer lugar, *el sistema de información en sí mismo* debe ser un instrumento, una herramienta que promueve la transformación organizacional *provocando una nueva exigencia de racionalidad, generando nuevas expectativas y estableciendo patrones de calidad que no puedan ser eludidos en el proceso de toma de decisión***"**(CEJA 2008).

Según otro estudio del CEJA[31], cuando se consideran las TIC como instrumento para mejorar el funcionamiento de la justicia, pese a los avances que han existido, en la Región existen aún vacíos profundos y quizá esfuerzos no bien orientados pese a la inversión realizada.

Para mencionar algunos de estos vacíos, se puede señalar que las TIC podrían tener un alto impacto en mejorar los niveles de transparencia en la operación de las instituciones del sistema de justicia, en mejorar el acceso de la ciudadanía al sistema de justicia, en aumentar los grados de eficiencia y eficacia en el desempeño de múltiples labores, en posibilitar y potenciar los procesos de innovación en la impartición de justicia y en la gestión judicial, en posibilitar la auditoria ciudadana sobre el sistema de justicia, en facilitar la rendición de cuentas de las autoridades judiciales a la ciudadanía, entre otros ámbitos.

Hay varios sectores de la administración de la justicia donde se pueden encontrar aplicaciones de las TIC. Entre ellos básicamente:

1. La reforma en los procesos penales, lo que solamente en los mejores casos ha traído avances en romper la tecnología de producción del expediente y pasar a una tecnología de producción basada en audiencias orales. Subsisten materias, principalmente las civiles, en que aún persiste la tecnología del expediente (Ej.: Brasil).
2. La organización de los tribunales de primera instancia, creando áreas comunes para notificaciones, recepción de documentos y archivos, entre otros, pero los tribunales de segunda instancia mantienen sus estructuras y funcionamientos habituales (Ej.: Chile, Uruguay, Perú).
3. La tramitación de casos, con lo que es posible informar más fácilmente al público sobre el estado de las causas, pero no han abandonado la lógica del expediente, por lo que las causas se siguen demorando mucho, pero al menos el público tiene acceso a la información respecto al estado se encuentra el caso.

Para tener un primer dato de cómo medir la relación entre los sistemas de Justicia (instituciones judiciales de varios niveles) y el uso de TIC, se escogió un dato general (cuadro 5 - índice de acceso a la información en Internet de los Tribunales) como índice de los sistemas judiciales ***hacia*** las TIC, y un indicador específico (cuadro 7 - publicación y actualización de sentencias) como dato para medir la presencia de los sistemas judiciales ***en*** las TIC.

El estudio de CEJA ha definido un conjunto de 25 indicadores para los Tribunales de Justicia, agrupados en 10 categorías (cuadro 6) que dan cuenta de las variables relevantes de lo que se ha estimado debería ser la información que los Tribunales proporcionan a los usuarios a través de Internet. Por cada categoría de indicadores se ha definido el peso relativo que ésta tendría dentro de un único índice global.

[31] Perspectivas de uso e impactos de las Tic en la Administración de Justicia en América Latina, CEJA 2008.

CUADRO 5
ACCESO A LA INFORMACIÓN EN INTERNET DE LOS TRIBUNALES DE JUSTICIA

	Index de acceso a la información en Internet de los tribunales de Justicia*
Argentina	65,9%
Bolivia (Estado Plurinacional de)	37,4%
Brasil	73,9%
Chile	77,8%
Colombia	46,4%
Costa Rica	75,0%
Cuba	/
Ecuador	35,9%
El Salvador	38,6%
Guatemala	26,1%
México	42,2%
Paraguay	31,0%
Panamá	66,8%
Perú	53,9%
Rep. Dominicana	79,6%
Uruguay	39,4%
Venezuela (República Bolivariana de)	62,1%

Fuente: CEJA 2008.
* El cuadro muestra las categorías evaluadas para los Tribunales de Justicia, su peso relativo respecto a la composición del índice, y el número de indicadores asociados a cada una de ellas.

CUADRO 6
IMPORTANCIA RELATIVA DE CADA CATEGORÍA CON RESPECTO A LA COMPOSICIÓN DEL ÍNDICE

Número categoría	Descripción	Peso relativo	N. de indicadores asociados
1	Existencia de página Web	5,0%	1
2	Publicación y actualización de sentencias	16,7%	4
3	Publicación y actualización de reglamentos	5,0%	1
4	Publicación de estadísticas de causas ingresadas, resueltas y pendientes	16,7%	4
5	Publicación de agenda de Tribunales	15,0%	1
6	Publicación de recursos físicos y materiales con que cuentan los tribunales.	5,0%	1
7	Presupuesto	16,7%	3
8	Salarios, antecedentes curriculares, patrimonio y temas disciplinarios de funcionarios relevantes.	10,0%	4
9	Publicación de concursos y licitaciones para contrataciones.	5,0%	3
10	Régimen de acceso y centralización de información	5,0%	3

Fuente: CEJA 2008.

CUADRO 7
PUBLICACIÓN Y ACTUALIZACIÓN DE SENTENCIAS EN INTERNET

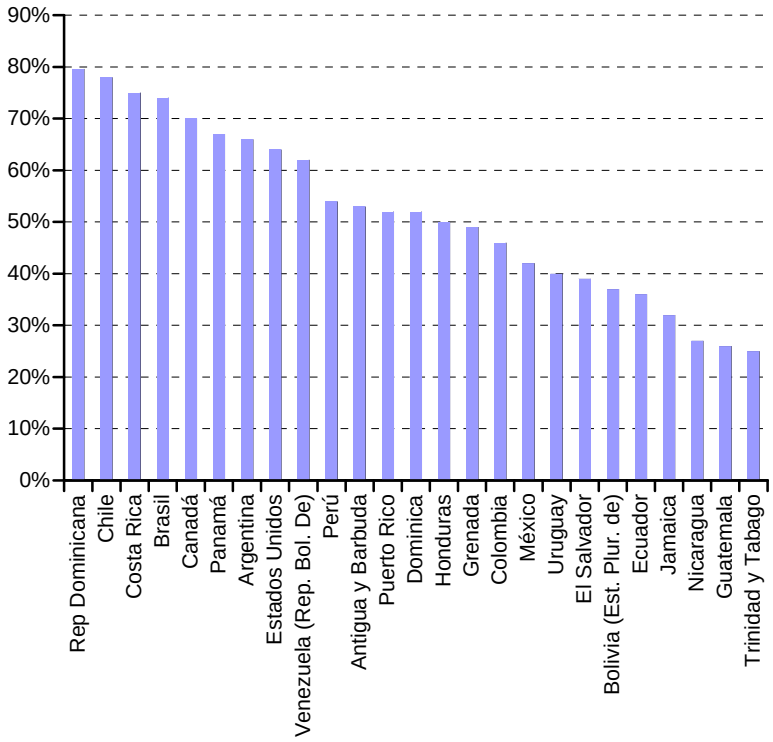
	Publicación y actualización de sentencias en Internet
Argentina	13,9%
Bolivia (Estado Plurinacional de)	11,1 %
Brasil	16,7%
Chile	5,5%
Colombia	12,5 %
Costa Rica	11,1 %
Cuba	-
Ecuador	11,1 %
El Salvador	15,3%
Guatemala	0,0%
México	0,0%
Paraguay	8,3%
Panamá	12,5 %
Perú	5,5%
Rep. Dominicana	11,1%
Uruguay	0,0%
Venezuela (República Bolivariana de)	16,7 %

Fuente: CEJA, 2008. Valoración de indicadores (CEJA): se publican sentencias de todos tribunales = 1; se publican sentencias de la mayoría de la materias = 0.67; se publican sentencias de la minoría de las materias = 0,33; no se publican sentencias = 0

De acuerdo a los datos presentados en los Cuadros 5 y 7 en algunos casos donde hay índices de acceso relativamente alto a Internet - **Chile, Perú** - no necesariamente los Tribunales demuestran usar el Internet para difundir informaciones con porcentajes elevados. De manera contraria, hay casos donde, si bien el acceso es más moderado (**Ecuador, Colombia**) se registra un nivel más alto de uso de Internet para dar información judicial, teniendo en cuenta las debidas proporciones.

Eso quiere decir que todavía el uso de las posibilidades de Internet *hacia fuera* (dar información *al* público*)* permanece en niveles moderados, más bien prevalentemente se trata de un uso *interno* a los Tribunales. También quiere decir, con buena aproximación, que hay casos de países con acceso/uso más moderado que demuestran saber aprovechar más los medios tecnológicos para informar a las personas interesadas.

GRÁFICO 8
ÍNDICE 2008 DE ACCESO A LA INFORMACIÓN DE TRIBUNALES DE JUSTICIA A TRAVÉS DE INTERNET



Fuente: CEJA – Índice de accesibilidad a la información judicial en Internet, cuarta versión, 2008.

Esta conclusión parece ser confirmada por otros resultados. Por ejemplo, si se considera el principal servicio online que se debería ofrecer al público, o sea la consulta de causas pendientes, haciendo un rápido análisis de los sitios Web de los Tribunales Superiores de Justicia, o donde no haya, de los sitios Web de los Poderes Judiciales, se puede estimar lo siguiente: de los países analizados en el cuadro 8, un 33% de sitios no ofrecen aun este servicio. Este dato índica la necesidad de mayores esfuerzos para que los ciudadanos puedan acceder a la información relativa a juicios pendientes sin tener la necesidad de presentarse físicamente en el Tribunal (cuadro 9).

CUADRO 9
PRESENCIA DE HERRAMIENTAS PARA VER EL ESTADO DE CAUSAS ONLINE DENTRO DE LOS SITIOS WEB DE TRIBUNALES DE JUSTICIA O DEL PODER JUDICIAL

	Presencia de herramientas	Sitios Web	Notas
Argentina	sí	http://www.csjn.gov.ar	
Bolivia (Estado Plurinacional de)	no	http://suprema.poderjudicial.gov.bo/	
Brasil	sí	http://www.stf.jus.br	
Chile	sí	http://www.poderjudicial.cl/	
Colombia	sí	http://www.ramajudicial.gov.co/csj_portal/jsp/frames/index.jsp?idsitio=3	

(continúa)

Cuadro 9 (conclusión)

Costa Rica	sí	https://pjenlinea.poder-judicial.go.cr/gestion/	Se encuentran también: formulario notificaciones electrónicas
Ecuador	no	http://www.cortesuprema.gov.ec	
El salvador	no	http://www.csj.gob.sv	
Guatemala	no	http://www.oj.gob.gt	Previsión de Juzgados móviles
México	sí	http://www2.scjn.gob.mx/expedientes/	
Panamá	sí	http://www.organojudicial.gob.pa/	
Paraguay	no	http://www.csj.gov.py:8080/portal	
Perú	sí	http://www.pj.gob.pe/	Se encuentran también: formulario notificaciones electrónicas; registro nacional de condenas
Rep. Dominicana	sí	http://www.suprema.gov.do/	
Uruguay	sí	http://www.poderjudicial.gub.uy	
Venezuela (República Bolivariana de)	sí	http://www.tsj.gov.ve	Amparo constitucional online

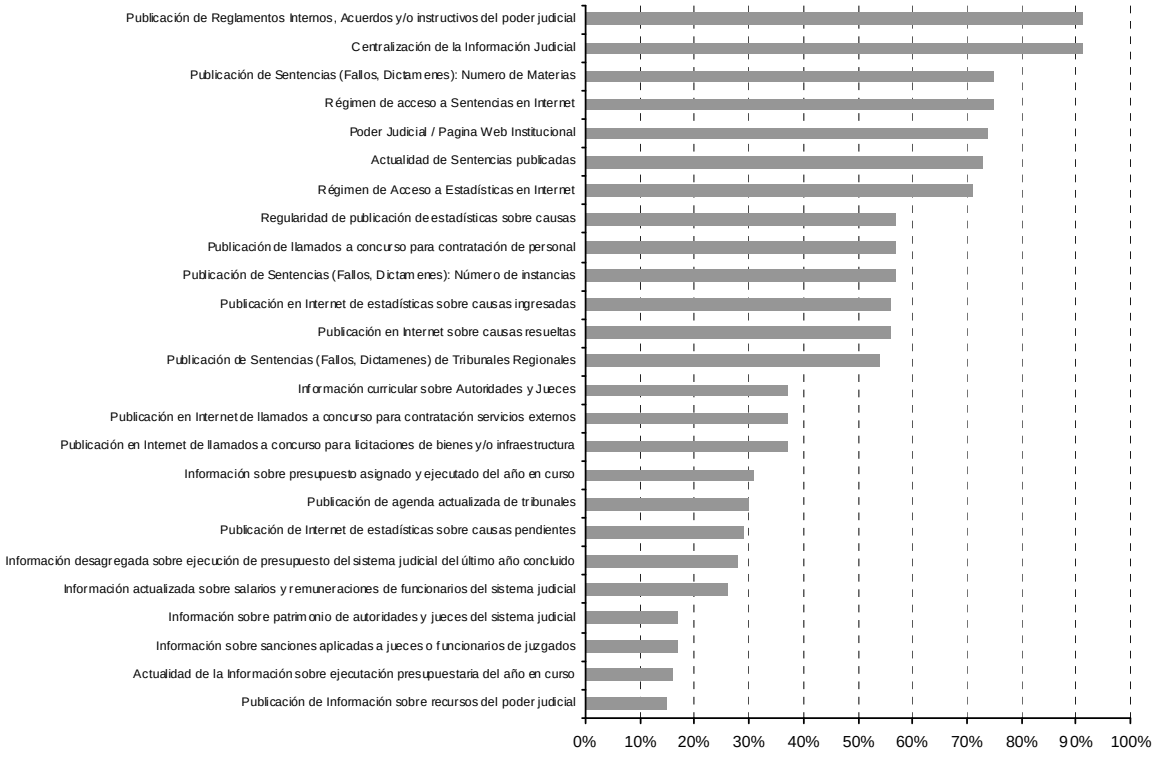
Fuente: elaboración propia.

Otro dato de interés es el acceso por tipología de indicador (gráfico 2), lo que explica mejor la conclusión anterior y permite averiguar en que forma la Web permite dar informaciones *hacia* el público. Los indicadores con valores más altos son la publicación de actos jurídicos (reglamentos), la publicación de sentencias y dictámenes de todo tipo.

Con referencia a este último punto, el dato no permite saber si se trata de acceso a procesos pendientes (servicio evidentemente más útil) o solamente de acceso a sentencias publicadas que corresponden a procesos ya finalizados. Cabe decir que en el primer caso se destacaría por ser un servicio muy novedoso y, por eso, al mismo tiempo, muy poco común, que necesita del traspaso de documentos desde el papel a formato digital, lo que, en procesos con mucha documentación, como son los procesos penales, se presenta como un desgaste de tiempo considerable.

Por el contrario, tienen valores muy bajos los indicadores que abarcan más bien la transparencia financiera de los Tribunales (ejecución presupuestaria, recursos del poder judicial) o la gestión del personal (sanciones aplicadas a jueces o funcionarios del poder judicial).

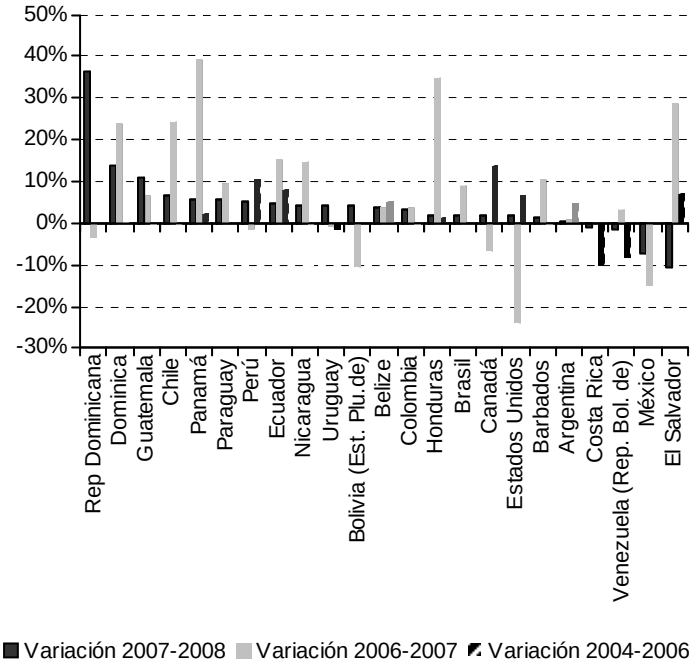
GRÁFICO 10
ÍNDICE 2008 DE ACCESO A LA INFORMACIÓN DE TDJ DE LAS AMÉRICAS A TRAVÉS DE INTERNET, POR INDICADOR



Fuente: CEJA – Índice de accesibilidad a la información judicial en Internet, cuarta versión, 2008.

Ahora bien, siguiendo con el análisis de los datos de acceso, resulta muy importante ver cuáles países se han destacado en el último periodo por usar más Internet en los Tribunales de Justicia. El Caribe y Centro América, en este sentido, demuestran los esfuerzos mayores. Cabe destacar también que hay países que presentan una variación negativa, entre ellos México y El Salvador (gráfico 11).

GRÁFICO 11
VARIACIÓN EN EL ÍNDICE DE ACCESO A LA INFORMACIÓN A TRAVÉS DE INTERNET EN TRIBUNALES DE JUSTICIA ENTRE 2004 Y 2008



Fuente: CEJA – Índice de accesibilidad a la información judicial en Internet, cuarta versión, 2008.

Los datos presentados destacan en parte el proceso de integración de los sistemas judiciales con las tecnologías, demostrando un camino en evolución que en general, en América Latina y el Caribe está dando señales positivas. Este proceso de desarrollo de una mayor transparencia en las informaciones que se refieren a la justicia puede ser afectado por la reivindicación de la debida independencia por parte de las instituciones judiciales. En algunos Tribunales, la necesidad de rendir cuentas, en particular, puede ser vista como una forma de limitación de la autonomía constitucionalmente garantizada a los poderes judiciales, y por ende en algunos casos la información online podrá aparecer limitadamente.

El desafío en este sentido es permitir que el escrutinio público sobre el sistema de justicia ayude a mejorar el servicio y alentar el proceso de apertura para aumentar la confianza de los ciudadanos en el poder judicial.

El *Informe Global de la Corrupción* 2007 de Transparency International[32], reveló que América Latina mostraba los niveles más bajos de confianza en el Poder Judicial, en tanto un 73% de las personas encuestadas en 10 países de América Latina manifestaron que el Poder Judicial era corrupto. La incapacidad de los sistemas judiciales para sancionar a quienes cometen delitos en algunos países fomenta la percepción de impunidad de los sectores poderosos, la sensación de inseguridad entre los ciudadanos comunes y un menor interés por parte de los inversionistas extranjeros.

Esta falta de confianza de los ciudadanos podría ser disminuida a través de un uso calibrado de tecnologías que aumenten el nivel de los servicios informativos al público y permitan una revisión frecuente, por parte de los usuarios, de las modalidades operativas de los Tribunales de Justicia en la Región.

[32] Transparency International "Los altos niveles de corrupción persistentes en países de bajos ingresos suponen un "desastre humanitario continuo", Documento sobre IPC (Índice de Percepción de la Corrupción) 2008, en http://www.transparency.org

Las buenas prácticas

En la sección precedente, se ha tratado el tema de la relación TIC – sistemas judiciales. Ahora bien, hay ejemplos de uso de las TIC para agilizar los procesos y brindar seguridad, rapidez, y ahorro de energía en el desarrollo de la actividad legal.

Lo primero a lo que es pertinente hacer referencia es la fase procesal, como la presentación de los actos escritos: demanda y la contestación de la demanda. Una mirada a la Unión Europea, por ejemplo, muestra que en Portugal y España es permitida la presentación por correo electrónico. En Inglaterra sólo para alegaciones por montos limitados (< 100 libras), mientras que en Italia no está previsto. Aquí la dificultad mayor no estriba en la infraestructura disponible sino en lo relativo a la autenticidad de los actos.

Las nuevas tecnologías incluso pueden ser aplicadas en la realización de los actos procesales orales. Es posible que estos se realicen mediante videoconferencia, pero ello no ha sido reconocido en la mayor parte de los ordenamientos jurídicos.

Pero para que ello funcione debidamente, deberían otorgarse determinadas garantías. Primeramente, será necesaria la constatación de la identidad de los sujetos que realizan los actos procesales. En segundo lugar, deberá respetarse el método contradictorio. Por lo tanto, deberá otorgarse la posibilidad de las partes a que se contradigan (por ejemplo en la interrogación de los testigos por parte de los interesados principales o en la misma declaración de partes, debe cada uno de los interesados y el Tribunal, ser parte de la videoconferencia).

En **Uruguay** hay un tipo de procedimiento que puede tramitarse por vía electrónica: el procedimiento administrativo[33]. El artículo 4 del decreto 65/998 establece que "*todas las normas sobre procedimiento administrativo serán de aplicación a los expedientes tramitados en forma electrónica, en la medida en que no sean incompatibles con la naturaleza del medio empleado"*, lo que es ampliado por el artículo. 5 del Decreto 65/998 al prescribir que "*toda petición o recurso administrativo que se presente ante la Administración podrá realizarse por medio de documentos electrónicos*".

Otro ejemplo es el de España, donde se fomenta el arbitraje *on line* para la solución de conflictos originados en relaciones de consumo. La Asociación Comunitaria de Arbitraje y Mediación, que opera en la Unión Europea, realiza también este tipo de procedimientos. La *American Arbitration Association* también los ha desarrollado mediante la instauración del *Virtual Magistrate Project*.

Un caso destacable en América Latina es el Cibertribunal peruano, órgano para la resolución de conflictos originados en el uso de Internet. El Cibertribunal peruano es un órgano de resolución de conflictos y controversias ocurridas en y por el uso de Internet que fomenta la Conciliación entre las partes y el Arbitraje como medio de resolución de conflictos y es competente en temas de Derecho Informático. Es un Centro de Conciliación acreditado por el Ministerio de Justicia y Centro de Resolución de Controversias entre nombres de dominio y marcas[34]. El procedimiento está previsto como sigue: una vez presentada la solicitud de arbitraje, el Cibertribunal peruano operará como un Centro de Arbitraje entre las partes. La comunicación entre los representantes del Cibertribunal peruano se desarrollará mediante correo electrónico. Las audiencias de arbitraje se realizarán utilizando en algunos casos el correo electrónico y en otros se aplicarán sesiones de *chat* y de vídeo conferencia entre las partes en conflicto y el Tribunal, así como entre los Vocales del Tribunal. Se usarán sistemas de encriptación que asegurarán la confidencialidad de las comunicaciones. Si la solicitud de arbitraje es presentada por una sola parte, se publica en la Página Web del Cibertribunal una reseña de la solicitud o demanda para alentar la respuesta de la contraparte. Finalizado el caso, se publica en la Página Web del Cibertribunal peruano un resumen de la resolución únicamente con el fin de crear precedentes.

Otra materia que ha permitido resultados exitosos, es la de la notificación electrónica de los actos. En **Uruguay** eso es posible en el ámbito administrativo. El artículo. 696 de la Ley N° 16.736 de 5 de

[33] Las Nuevas Tecnologías Aplicadas al Proceso Jurisdiccional y en Particular la Prueba Digital en el Derecho Uruguayo Vigente, Santiago Madalena Solimano, en www.alfa-redi.org

[34] http://www.cibertribunalperuano.org

enero de 1996 prevé que "*la notificación personal de los trámites y actos administrativos podrá realizarse válidamente por correo electrónico u otros medios informáticos o telemáticos, los cuales tendrán plena validez a todos los efectos siempre que proporcionen seguridad en cuanto a la efectiva realización de la diligencia y a su fecha*". Con una mirada al derecho comparado, el sistema de notificación por correo electrónico ya se ha incorporado con éxito en países de América Latina (**Costa Rica**, **Perú**, algunas **provincias argentinas**) y europeos. La mayor limitación a que mecanismos como éste se estructuren, viene dada por la infraestructura disponible. Sin embargo, no parece algo tan lejano si es instaurado mediante proyectos pilotos, o en forma moderada, y paulatina, empezando por ejemplo por los abogados. Evidentemente, deberá ser reglado de manera eficiente para evitar la indefensión. Fuera del ámbito procesal, ya se han implementado las comunicaciones de los órganos gubernamentales al público en general a través de sus páginas Web.

Sin duda entre las buenas prácticas en la Región se hace notar el caso de **Brasil** (cuadro 12).

La *Ley de Informatizaçao do Processo Judicial* n. 11.419/2006, y las siguientes modificaciones (Resolución n 341/2007, Resolución 357/2007, Resolución 344/2007) han introducido una gran cantidad de innovaciones en el sistema jurisdiccional brasilero en el uso de las tecnologías.

Brevemente:

1. la creación del Diario de Justicia Electrónico (Abril 2007 - Ley 11419/06);
2. el uso de certificación digital, autenticidad integridad e interoperabilidad de los documentos electrónicos asignados con certificados digitales emitidos para la infraestructura de Llaves publicas Brasileñas - ICP;
3. el Recurso Extraordinario Electrónico, conocido como RE electrónico para el traspaso de material probatorio al Supremo Tribunal Federal (objetivo de reducir marcadamente el número de material en papel que llega a los Tribunales). Desde el 2007 está funcionando regularmente el e-Pet, servicio que permite la petición electrónica de todo tipo de documentos en los Tribunales.
4. citación electrónica prevista por el Código Civil bajo dos condiciones: a) previa registración de los usuarios en el Portal del Poder Judicial ("*credenciamento no Poder Judiciário*"), b) acceso para entrega de los actos por parte de la persona citada;
5. en el Proceso Electrónico todas las Citaciones deben ser hechas por medio electrónico, cuando no sea posible deberá ser realizada según las reglas ordinarias, a través de la digitalización del documento físico que será posteriormente destruido (para ahorro de papel y menor gasto de justicia);
6. iniciación electrónica (acto con el cual se deja saber a alguien que tiene que dejar de hacer una cosa o que tiene que empezar a hacerla).

CUADRO 12
BRASIL – BUENAS PRÁCTICAS EN MATERIA DE E-JUSTICIA

Nombre	Responsable	Descripción	Lugar de implementación	Resultados
Proceso Virtual	Tribunal de Justiça do Distrito Federal (TJDF)	Digitalización de todos los procesos en trámite en las ocho zonas de Juzgados Especiales Civiles de la zona de Brasilia. En la segunda etapa, la meta es expandir la digitalización a los Juzgados Especiales Civiles de todas las zonas de DF.	Zonas de los Juzgados Especiales Civiles de DF	Economía de papel – las principales documentaciones de procesos son almacenadas en un banco de datos virtual. El archivo virtual reduce costos y garantiza mayor seguridad en el almacenamiento de las informaciones.

(continúa)

Cuadro 12 (conclusión)

Proyecto de Digitalización de Audiencias	Tribunal de Justiça do Distrito Federal (TJDF)	El proyecto tiene por finalidad el registro digital (grabación de audio y video) de las audiencias realizadas en el curso de los procesos, posibilitando la pronta recopilación en cualquier momento.	Inicialmente, las grabaciones de las audiencias ocurren en el 9o Juzgado Civil de Brasilia. Esto ocurre en convenio con la Universidad de Brasilia (UnB) junto con recursos privados.	La digitalización posibilita verificar, en cualquier tiempo y jurisdicción, el desarrollo de las audiencias realizadas en primera estancia. Para la grabación, se da pleno acceso a las partes y los abogados a todo el material probatorio producido.
Interrogatorio On-Line	Tribunal de Justiça do Distrito Federal (TJDF)	La tecnología permite al juez interrogar al reo preso, para cumplir la pena, sin que el mismo se desplace hasta el juzgado. Un monitor de vídeo es instalado en una sala del presidio local, mientras que el otro monitor funciona en la sala del juez, que se comunicará con el preso virtualmente. A finales de la sesión, el resultado de la audiencia es impreso y firmado por el preso.	Lugares de Juzgados Penales de Brasilia	Economía en cuanto al traslado del preso. Más agilidad del proceso penal
Autentificación virtual de certifica-dos de antecedentes criminales	Tribunal de Justiça do Pará (TJ-PA)	Verificación de antecedentes criminales a través del sitio Web del Tribunal	Tribunal de Justiça do Pará (TJ-PA)	Agilidad del servicio para los ciudadanos
Acompañamiento virtual a los procesos	Juzgado de la zona 1 de Aras (São Paulo)	Creación de un *software* para facilitar el seguimiento de los procesos por parte de los actores del mismo - y los abogados -	Juzgado de zona 1 de Aras	Garantiza independencia física de los abogados en los procesos que pueden ser seguidos directamente a través de un computador
Optimización del sistema de intimación personal	Juzgado Especial Civil de Florianopolis (SC)	Sistema de intimación electrónica de sentencias, decisiones con obligación de los abogados de inscribirse en la página de la Sección Judiciaria de SC	Juzgado Especial Civil de Florianopolis (SC)	El 100% de los abogados inscritos en el Juzgado está registrado para el procedimiento

Fuente: Elaboración propia.

Otro ejemplo interesante es el caso de los tribunales penales de garantías en **Chile**.

Los tribunales de garantías en materia penal de Chile, desde su creación e implementación gradual en diciembre de 2000 hasta junio de 2005, han ido incorporando continuas mejoras en materia de gestión. Entre ellas, la interconexión con el sistemas informático del Ministerio Público, la eliminación gradual de la carpeta física de cada caso judicial, la recepción de documentos de las partes sólo por vía electrónica, las que han funcionado basadas en principios de confianza y buena fe, ya que aún no está disponible la firma electrónica de documentos, entre otros. Desde mediados de 2006, se han dictado actos acordados de la Corte Suprema para abandonar el papel y tramitar todos los casos en forma electrónica.

VI. Glosario de términos utilizados

CUADRO 13
GLOSARIO DE TÉRMINOS UTILIZADOS

	Definición	**Fuente**
Firma electrónica	Cuándo un símbolo o una serie de símbolos, ejecutados, adoptados o autentificados por parte de una persona para que sean equivalentes a la propia firma manual, se convierten a formato digital (*the entry in the form of a magnetic impulse or other form of computer data compilation of any symbol or series of symbols, executed, adopted or authorized by a person to be the legally binding equivalent of the person's handwritten signature*)	U.S. Federal Register, 20 Marzo 1997 (21 CFR Part 11 Electronic Records; Electronic Signatures; Final Rule) www.isaacbowman.com/electronic-signatures-in-global-and-national-commerce-act-esign
Public key Infrastructure (infraestructura de clave publica)	Transmisión segura de datos y sistema de autenticación que utiliza una criptografía de clave pública *(Secure data transmission and authentication system that uses public key cryptography (PKC))*	The Business dictionary.
Public key cryptography (criptografía de clave pública)	Esquema de trasmisión segura de datos usada en *pretty good privacy.* También llamada encriptación no secreta, que se presenta diferente de la criptografía de clave simétrica donde tanto el que recibe como el que envía tienen la misma clave electrónica. Desarrollada en 1976 por Whitfield Diffie y Martin Hellman de EE.UU. (*Secure data transmission scheme used in pretty good privacy (PGP). Also called non-secret encryption, PKC is different from symmetric key cryptography where both sender and receiver have the same electronic key. Developed in 1976 by Whitfield Diffie and Martin Hellman of the US)*	The Business dictionary.
Comercio electrónico	Consiste en realizar electrónicamente transacciones comerciales; es cual-quier actividad en que las empresas y los consumidores Interactúan y hacen negocios entre si o con las administraciones por medios electrónicos.	comunicación de la Comisión Europea al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las regiones - Iniciativa europea de comercio electrónico - COM/97/0157 final

VII. Bibliografía

Altmark, Daniel Ricardo, (1987) *Informática y Derecho*, vol. 1, Depalma, Buenos Aires.

A. Riquert, Marcelo, (2008) *Algo más sobre la Legislación contra la Delincuencia Informática en MERCOSUR a propósito de la Modificación al Código Penal Argentino por Ley 26388.*

Bellver, Ana, (2007), *Reformas en materia de transparencia: segunda generación de cambio institucional*, Revista del CLAD.

BID (2005) *E-Congreso. El Poder Legislativo en la era de la información: una oportunidad para la acción*, Washington.

Castells, Manuel, (1996), La era de la información: economía, sociedad y cultura, vol. 1, La sociedad Red, Alianza Madrid, pp. 57-58.

__ (2001) "Internet, libertad y sociedad: una perspectiva analítica", Conferencia inaugural del curso académico 2001-2002 de la UOC.

Castillo Jiménez, María Cinta, Ramallo Romero, Miguel, (1989) "*El delito informático"* Facultad de Derecho de Zaragoza. Congreso sobre Derecho Informático. 22-24 junio.

CEJA, (2008), *Perspectivas de uso e impactos de las Tic en la Administración de Justicia en América Latina*, www.cejamericas.org.

CEPAL, (2008), *Monitoring eLAC2007: progress and current state of development of Latin American and Caribbean information society.*

Chadwick, A. and May, C. (2003) "Interaction between States and Citizens in the Age of the Internet: 'e-Government' in the United States, Britain and the European Union, *Governance: An International Journal of Policy, Administration and Institutions* 16(2): 271-300.

Corrales, Marcelo (2008) *E-signatures in MERCOSUR* , www.alfa-redi.org.

Dalla Riva, Giovanni (2002) *"El problema de la firma digital"*, Editorial Universitaria, Zaragoza.

Daniel Peña Valenzuela, (2003), *Lex Electrónica: Mito o Realidad? Perspectiva desde la contratación por medios electrónicos* in *La Propiedad Inmaterial,* Revista del Centro de Estudios de la Propiedad Intelectual de la Universidad Externado de Colombia, Nro. 7, pag. 103.

Dunleavy, P., Margetts, H. (2000) "*The Advent of Digital Government: Public bureaucracies and the state in the information age*", Annual Conference of the American Political Science Association, Washington.

Gallego Higueras Gonzalo F. (2002), *Código de Derecho Informático y de Las Nuevas Tecnologías*, Civitas, Madrid.

Jordan Flores, Fernando (2000), *Las Nuevas Tecnologías, el Derecho y la Justicia*, Servigraphic, LTDA, Colombia.

Lindstedt Catharina, Naurin Daniel (2008), *Transparency against Corruption. A Cross-Country Analysis.*

Kaufman, Ester (2005) "*E-ciudadanía, Practicas de buen Gobierno y TIC"*, Documento preparado para la consulta regional del Programa Pan Américas IDRC .

Madalena Solimano, Santiago, (2007) Las Nuevas Tecnologías Aplicadas al Proceso Jurisdiccional y en Particular la Prueba Digital en el Derecho Uruguayo Vigente, en www.alfa-redi.org.

Mata y Martín, Ricardo M. (2001), *Delincuencia Informática y Derecho Penal,* Editorial Edisofer, Madrid.

Moreno Escobar H., (2007) "*Modelo multi-dimensional de medición del gobierno electrónico para América Latina y el Caribe, proyecto Sociedad de la Información*", CEPAL, Naciones Unidas, Santiago.

__ (2009 en publicación), *El fin del gobierno electrónico. Transformación para un buen gobierno*. Proyecto Sociedad de la Información, CEPAL, Naciones Unidas, Santiago de Chile.

Orts Berenger, Enrique y Roig Torres, Margarita, (2001) *Delitos informáticos y delitos comunes cometidos a través de la informática*, Editorial Tirant Lo Blanch, Valencia.

Pérez Luño, Antonio Enrique, (1996), *"Manual de informática y derecho"* Editorial Ariel S.A., Barcelona.

Peters, B.G. and Pierre, J. , (1998), *Governance without Government? Rethinking Public Administration*, Journal of Public Administration Research and Theory 8(2):223-243.

Romeo Casabona, Carlos María (1987) "*Poder informático y Seguridad jurídica*", Editorial Fundesco.

Ríofrio Martínez-Villalba Juan Carlos (2002)**,** *La Pretendida Autonomía del Derecho Informático,* Revista de Derecho Informático 50 (2002).

Ruiz Marco, Francisco, (2001) *Los delitos contra la intimidad, Especial referencia a los ataques cometidos a través de la Informática,* Editorial Colex.

Sunga, Lyal S. (1997) *The emerging system of international criminal law: developments in codification and implementation*, The Hague, Kluwer Law International.

Stephen Mason (2007), *Electronic Signatures in Law* (Tottel, second Edition).

Téllez Valdés, Julio, (2003) *Derecho Informático*, 3ª ed., Ed. Mac Graw Hill, México.

Transparency International (2008), "*Los altos niveles de corrupción persistentes en países de bajos ingresos suponen un desastre humanitario continuo*", Documento sobre IPC (Índice de Percepción de la Corrupción), en http://www.transparency.org.

Williams Phil, (2001) "*Organized Crime and Cybercrime: Synergies, Trends, and Responses*", International Information Programs, Electronic Journal of the U.S. Department of State – August 2001 Volume 6, Number 2.

Wimmer M., and Traumuller, R., (2001) *Electronic Business invading the Public Sector: consideration on change and design*, 34th Hawaii International Conference on System Sciences (HICSS), Hawaii.