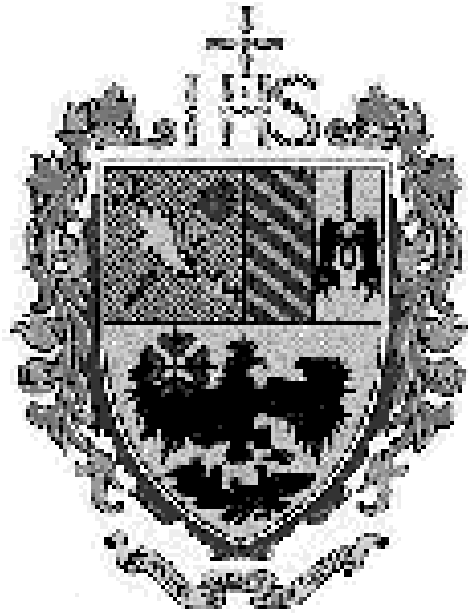


**UNIVERSIDAD DEL SALVADOR**  
FACULTAD DE CIENCIAS DE LA ADMINISTRACION

**MASTER EN DIRECCIÓN DE EMPRESAS**



**EL DERECHO ARGENTINO EN LA ERA DE LOS NEGOCIOS  
DIGITALES**

Por

Lic. Marcelo CATTANI  
Lic. Walter CORREA  
Lic. Juan ALZUGARAY  
Lic. Iván CASTANY

**Profesor: Dr. Horacio FERNÁNDEZ DELPECH**

Buenos Aires, 15 de septiembre de 2006

## **Aclaración**

Los puntos de vista expresados en el presente trabajo académico son exclusivos de los autores y no reflejan necesariamente políticas oficiales ni posición de la Universidad del Salvador ni de la Cátedra de Derecho Empresario.

## *Tabla de Contenidos*

ACLARACIÓN.....	II
PREFACIO.....	V
EXTRACTO.....	VI
INTRODUCCIÓN .....	1
TECNOLOGÍA Y COMERCIO ELECTRÓNICO .....	1
LA INFORMACIÓN .....	1
UNA NUEVA ECONOMÍA DIGITAL.....	2
EL COMERCIO ELECTRONICO .....	3
¿REVOLUCIÓN O ACELERADA EVOLUCIÓN?.....	3
LA GESTIÓN DEL CONOCIMIENTO .....	4
EL DÉFICIT CULTURAL DE LOS DIRIGENTES.....	4
LA CUESTIÓN EN PAÍSES EN DESARROLLO .....	4
CAPÍTULO I.....	5
ALCANCES TECNOLÓGICOS Y EL MARCO REGULATORIO .....	5
A SOLA FIRMA.....	5
LA FIRMA DIGITAL EN LA NORMATIVA ARGENTINA, EL DECRETO 2628/2002 COMO REGLAMENTACIÓN DE LA LEY DE FIRMA DIGITAL .....	9
EL DECRETO 2628/2002.....	11
LAS FORMAS DE EXPRESAR LA VOLUNTAD DIGITALMENTE.....	11
LAS COPIAS DE LOS DOCUMENTOS DIGITALES FIRMADOS.....	12
EL ESTÁNDAR TECNOLÓGICO: LA CRIPTOGRAFÍA DE CLAVE ASIMÉTRICA .....	12
EL ARANCELAMIENTO DE LA FIRMA DIGITAL .....	13
LA OBTENCIÓN DE LA LICENCIA COMO PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN .....	13
LOS CERTIFICADOS DIGITALES EMITIDOS EN EL EXTRANJERO.....	13
LA AUTORIDAD DE REGISTRO.....	14
LA NORMATIVA REFERIDA A LOS CONTRATOS DE CONSUMO.....	14
COROLARIO DEL CAPÍTULO .....	17
CAPÍTULO II.....	18
¿QUE PROVEE EL DERECHO EN LA ERA DIGITAL? .....	18
PROTECCION DE DATOS PERSONALES .....	18
PROPIEDAD INTELECTUAL.....	19
CORREO ELECTRONICO .....	20
COMERCIO ELECTRONICO.....	22
CONTRATOS.....	25
DEFENSA AL CONSUMIDOR .....	25
LEALTAD COMERCIAL .....	26
NOMBRES DE DOMINIO .....	26
RESPONSABILIDAD CIVIL.....	28
COROLARIO DEL CAPÍTULO .....	28
CAPÍTULO III .....	29

MARCO LEGISLATIVO Y PROYECTOS .....	29
LEGISLACIÓN Y PROYECTOS .....	29
COMERCIO ELECTRONICO.....	29
DECRETO 724/2006 .....	32
COROLARIO DEL CAPÍTULO .....	33
CAPÍTULO IV .....	34
CONCLUSIONES .....	34
ARGENTINA EN LA ERA DE LOS NEGOCIOS ELECTRÓNICOS.....	34
COORDINACIÓN NORMATIVA INTERNA E INTERNACIONAL (MERCOSUR).....	35
LA REINVENCIÓN DE LAS EMPRESAS .....	35
PERSPECTIVAS DEL COMERCIO ELECTRÓNICO.....	36
EL ROL DEL GOBIERNO: LIDERAR EL CAMBIO .....	37
PROPULSAR A LAS TIC .....	38
GLOSARIO DE TÉRMINOS .....	40
BIBLIOGRAFÍA .....	41
LIBROS .....	41
ARTÍCULOS .....	41
SITIOS WEB .....	41
ANEXO “A”.....	I-1
ARTÍCULOS PERIODÍSTICOS.....	I-1
ANEXO “B”.....	II-1
LEYES Y DECRETOS .....	II-1
FIRMA DIGITAL.....	II-1
LEY DE FIRMA DIGITAL .....	II-1
FIRMA DIGITAL, DECRETO 724/2006.....	II-14

## *Prefacio*

En Agosto de 2000, el Gobierno argentino comenzó a dar señales de haber comprendido la importancia de comprometer al país en el desarrollo de las nuevas Tecnologías de la Información y Comunicaciones (TIC).

El Decreto del Poder Ejecutivo Nacional 252/2000 dio creación al Programa Nacional para la Sociedad de la Información, y posteriormente se creó el Comité Argentina Digital, presidido por el entonces Vicepresidente de la Nación Lic. Carlos Alvarez, el Secretario de Ciencia y Tecnología y el Secretario de Comunicaciones. En ese entonces, con un criterio de integración se lanzó un plan de diseminación de computadoras personales (PC) - retomado en el actual Gobierno – y se concretaron importantes medidas en torno a la desregulación del mercado telefónico del país, lo que redundó en un incremento de la conectividad en redes ya existentes desde mediados de los noventa.

Existió entonces un enfoque sobre el desarrollo de las TIC exclusivamente basado en Internet, omitiendo importantes aspectos como la integración de segmentos como el Ministerio de Economía, el de Infraestructura y en general las estructuras exportadoras del país. Este comienzo embrionario desde el Estado Nacional y la carencia de recursos genuinos, un marco legal en desarrollo e ideas claras, privaron a las TIC del ímpetu que necesitaban para instalarse en nuestra sociedad.

De este modo, la Argentina llega al Siglo XXI sin una iniciativa o plan coherente, cuya falta de efecto se radica más allá de los niveles directivos del país que desconocen el fenómeno que se está viviendo y el impacto que producirá en todos los órdenes de la vida, fallando en la tarea de crear y sostener los medios propicios para el desarrollo. Esta falta de iniciativa se radica más allá del costo o limitación del ancho de banda. Esta falta de iniciativa se radica en la falta de ideas y trabajo corporativo.

Qué responsabilidad le cabe al atraso legislativo en la materia? El vacío legislativo es una consecuencia de la carencia de iniciativa que deviene en iniciativas legislativas contradictorias por falta de madre.

Este trabajo pretende establecer un cuadro de la situación actual y su relación con los negocios, motor del crecimiento de un Estado, pretende establecer una pintura de la posición digital de la Argentina en el Siglo XXI.

## *Extracto*

Los temas desarrollados en este trabajo comienzan con una introducción a las tecnologías de la información, el comercio electrónico y plantea la cuestión en los países en desarrollo referente al marco legal necesario para generar una verdadera infraestructura digital.

Analiza luego aspectos relacionados con los alcances tecnológicos y el marco regulatorio, las leyes relacionadas con la infraestructura digital (firma digital y defensa del consumidor) e intenta explicar las tecnologías implícitas.

Continúa con una revisión de que puede operacionalizar el derecho en el marco legal actual, se revisan las leyes y proyectos de ley en vigencia al día de la fecha, para tomar una noción del desarrollo legal que sustenta la infraestructura digital.

Por último se desarrollan las conclusiones referidas a una Argentina digital afrontando el Siglo XXI desde un fracaso para transformarse económicamente y desarrollarse.

Se agregan como elementos de juicio, artículos periodísticos y las leyes y decretos más importantes para la gestión de una infraestructura digital.

## INTRODUCCIÓN

### **Tecnología y Comercio Electrónico**

*“El hecho de que no podamos ver claramente el final del camino no constituye un impedimento para emprender el viaje. Por el contrario, el mundo está marcado por el cambio, y a menos que nos movamos en el cambio, nos convertiremos en sus víctimas”.*

***Robert F. Kennedy***

### LA INFORMACIÓN

1. La información es algo vital en toda organización, sin embargo algunas empresas deben esforzarse para poder ofrecerles los datos correctos a las personas indicadas, en el tiempo estipulado para la toma adecuada de decisiones poniendo especial atención a los puntos estratégicos, que de no ser correctamente administrados generan, demoras e imprecisiones.
2. Luego surgen las aplicaciones operacionales y empresariales, repartiéndolas a una variedad de interfases de usuarios, entre los que se incluyen los reportes, tableros de control, documentos de Office y portales. Los reportes posibilitan a las organizaciones formatear y enviar datos como información significativa a un gran número de usuarios, tanto dentro como fuera de la organización.
3. En las oficinas se realizan muchas tareas de forma simultánea y continua, por lo que hacer un seguimiento de la documentación adjunta puede ser mas complicado a medida que aumenta el volumen de documentos en papel. Con un software adecuado se puede almacenar archivos electrónicos, el flujo de trabajo, gestión de documentos y registros. Pero se necesita contar con una adecuada Seguridad Informática y con una legislación para poder ser respaldados ante la Ley.
4. Hoy somos todos protagonistas de una Revolución Tecnológica que esta cambiando la forma de comunicarnos, y a la vez somos espectadores de la lucha existente entre las grandes empresas de telecomunicaciones por quedarse con la mayor parte del

mercado.

5. Los avances de la tecnología, de la cibernética y de la robótica nos acercan cada vez mas a un mundo digital y automatizado, un escenario que sin lugar a dudas nos simplifica la vida cotidiana, pero que también nos lleva a un cambio de paradigma y en consecuencia a un reacomodamiento de nuestro rol.

6. Entre el film Inteligencia Artificial y el del Yo Robot pasaron no más de 20 años. Cuando en la película de Ridley Scott se relata la convivencia con seres cibernéticos se veía como un verdadero cuento de ciencia ficción, sin embargo hoy no son fantasías tan lejanas e irrealizables, tal vez pueda parecer exagerado, pero no imposible.

7. Todo cambio provoca un grado de inestabilidad y hasta de inseguridad. Mantener una corriente de información actualizada y un alto grado de conectividad en todo lo referido al universo tecnológico se ha convertido en parte estratégica del ejecutivo de hoy, teniendo especial importancia la convergencia tecnológica de los servicios y equipos wireless, las fusiones de las compañías de telecomunicaciones, la llegada de la telefonía IP y los nuevos hábitos de consumo de los navegantes a partir de las diversas maneras de acceder a Internet.

### **UNA NUEVA ECONOMÍA DIGITAL**

8. La economía tradicional se ha referido siempre a bienes tangibles en tanto que la nueva economía digital es básicamente, una economía de bienes inmateriales, de ideas. La economía es la ciencia de la escasez: en el mundo físico nadie puede usar la misma cosa al mismo tiempo, por ello los bienes son escasos. Pero, en cambio, ello es posible en el mundo digital. No sólo al mismo tiempo, sino para siempre, sin desgastarla. Y sin costos de distribución, o algo ínfimo (la distribución en INTERNET no cuesta nada).

9. La economía siempre ha luchado por la transparencia de los mercados en la búsqueda del mercado perfecto, y esta aspiración de Adam SMITH de los mercados perfectos y transparentes, se concreta con la red global que permite no solamente llegar a un mercado universal con transparencia casi perfecta y con reducidos costos de intermediación. La economía gira en derredor de un concepto, el de la moneda, que aparece sacudido por la posibilidad de creación de la moneda electrónica.

10. Todos estos presupuestos están ahora de alguna forma controvertidos o desafiados por la nueva realidad, y quizás autorizan a hablar de una nueva economía.

### **EL COMERCIO ELECTRONICO**

11. La importancia del Comercio Electrónico, el cual fue un acontecimiento totalmente inesperado, fue un impacto verdaderamente revolucionario aunque la revolución de la información recién esta comenzando a percibirse. No es la información la que alimenta este impacto, ni la inteligencia artificial, ni la influencia de las computadoras ni el procesamiento de datos en la toma de decisiones, es algo que prácticamente nadie previó, el comercio electrónico. A través del comercio electrónico se desarrolla el más importante canal de distribución mundial de productos y servicios movilizand o una parte importante de la economía mundial.

12. Esto esta cambiando radicalmente las economías, los mercados y las estructuras de la industria, la segmentación de clientes, los valores y el comportamiento del consumidor, los puestos de trabajo y los mercados laborales, lo que originará el surgimiento de de industrias nuevas e inesperadas y de otros modelos laborales.

13. Bajo estos aspectos, el desarrollo del derecho vinculado al comercio y empleo de las TIC es una condición mandatoria en las sociedades modernas, el individuo debe ser cuidado, el trabajador amparado, las comunicaciones protegidas y los negocios asegurados, ya que no hay desarrollo posible sin seguridad.

### **¿REVOLUCIÓN O ACELERADA EVOLUCIÓN?**

14. La discusión de si nos encontramos frente a una 'revolución' o a una drástica evolución no tiene mayor sentido si se coincide que enfrentamos un fenómeno que provoca cambios profundos que comprenden la vida en sociedad, los individuos, la cultura, y la economía.

15. Una cuestión central es la convergencia tecnológica que se verifica en forma diferente a la de los '70 y comienzos de los '80 entre las computadoras y las comunicaciones, pues ahora las computadoras personales permiten diseminar la información digitalizada, combinando un sistema multipropósito de comunicaciones (e mail) con la información

multimedia (en la Web) en una sola plataforma.

### **LA GESTIÓN DEL CONOCIMIENTO**

16. La economía industrial marcha hacia la economía de la información basada en el conocimiento. La nueva economía se basa en el intercambio de intangibles - ideas, información, conocimiento, inteligencia -. Los términos economía basada en el conocimiento, economía digital, sociedad de la información, etcétera, aluden a la sociedad del siglo XXI muy diferente de la sociedad industrial que prevaleció durante los últimos dos siglos en el mundo desarrollado.

### **EL DÉFICIT CULTURAL DE LOS DIRIGENTES**

17. El ingreso de la Argentina en la Era Digital debe hacerse de la mano de la clase dirigente, de los directivos de instituciones y organizaciones de todo tipo. Si éstos no lo asumen, dicho ingreso se producirá tarde y, una vez más, la Argentina estará perdiendo una gran oportunidad.

### **LA CUESTIÓN EN PAÍSES EN DESARROLLO**

18. Todo lo relativo a las TIC es particularmente aplicable a países en desarrollo. No sólo esto es cierto, sino que debería agregarse que quedarse quietos puede significar un retraso importante. Además, debe enfatizarse que los gobiernos de estos países tienen un importante rol a cumplir en la promoción de las TIC ya que se considera que el desarrollo de las mismas hace a la competitividad del país.

## CAPÍTULO I

### **Alcances Tecnológicos y el Marco Regulatorio**

#### **A SOLA FIRMA**

19. La sociedad actual tiene su principal basamento en las nuevas tecnologías de la información y las comunicaciones. Es indudable el aporte de estos dos componentes -ya inevitables- en la vida diaria actual. Tampoco se puede dudar de las ventajas que le aportan a las actividades económicas, sociales, culturales y políticas que ya no las ignoran, y mucho menos las desaprovechan.

20. Observando el impacto que dichas tecnologías provocan a la llamada Sociedad de la Información, cabe hacer algunas reflexiones. El futuro desarrollo de los servicios de información y telecomunicaciones, tales como servicios de enlaces móviles, compra electrónica, correo electrónico, servicios bancarios electrónicos, depende de una estructura segura de TIC, que no atente contra la confianza en esos servicios.

21. Bien es sabido la facilidad con que las nuevas tecnologías y sistemas pueden almacenar, distribuir y proporcionar datos relativos a las personas, invadiendo o al menos amenazando la esfera privada, el ámbito íntimo, lo que ha provocado la reactivación del conflicto individuo-sociedad, que se ve reflejado en la aparición de toda una serie de leyes de protección de datos personales y derecho a la privacidad.

22. Además, a pesar de los abusos que el sector privado pudiera cometer, normalmente los ciudadanos perciben al Estado como la amenaza mayor a su derecho a la privacidad. La doble percepción del Estado como amenaza y a la vez como garante de derechos, tiene fuertes implicaciones en la discusión del uso de las tecnologías en general y de las criptográficas en particular.

23. En el ambiente de los que trabajan, discuten o reflexionan sobre la seguridad de los sistemas de información y comunicaciones, se está de acuerdo en que la criptografía es una tecnología imprescindible para garantizar la confidencialidad, integridad y autenticidad

dentro de la infraestructura actual, y que esa garantía y protección es hoy vital para la existencia de los servicios de ámbito económico y financiero (aunque no se restringe a ellos) que se apoyan en la mencionada infraestructura.

24. Volviendo al Estado, mucho camino se ha recorrido desde el primer decreto que instauró en la Argentina el uso de la Firma Digital en su propio ámbito. Sin embargo, no ha sido suficiente el esfuerzo de los profesionales, para quebrar los intereses políticos que aún hoy impiden que se plasme la tecnología en realidad, no por la tecnología en sí misma sino por el sustento legal que requiere, sus aspectos de control e instrumentación. Sin embargo, en algún momento se debe tener vigente la plataforma legal que sustenta la denominada Infraestructura de Clave Pública. ¿Y luego qué?.

25. ¿Dónde están las aplicaciones? ¿Cómo integrarlas? ¿A cuáles procesos aplicarlas? Pues bien, allí comienza la rueda nuevamente. Observando rápidamente los problemas que plantea la sociedad digital y más aún los problemas derivados de esta, hay cientos de aplicaciones que requieren de identificación sin lugar a dudas y que de cara a la legislación proveerán valor probatorio. Los puntos clave surgen de estos aspectos fundamentales:

- 1º) Estandarizar, identificar sin lugar a dudas a personas y organizaciones y “despapelizar”.
- 2º) La estandarización se basa en la generación de políticas, normas y procedimientos para todos los ámbitos involucrados.
- 3º) La identificación sin lugar a dudas de las personas y organizaciones, se sustenta en la firma digital, que opera bajo la denominada Infraestructura de Clave Pública.
- 4º) La “despapelización”, como resultado de la utilización de la firma digital, da origen al Documento Digital, garantizando la autenticidad, integridad, no repudio y eventualmente la confidencialidad del mismo.

26. Es así que en este tiempo, es aplicable entre otras a las siguientes áreas:

### **Identificación e información**

- 1º) Identificación como usuario ante redes internas o externas (abiertas o cerradas).
- 2º) Correos electrónicos.
- 3º) Identificación de sitios en Internet.

- 4º) Comercio electrónico.
- 5º) Transacciones EDI (Electronic Data Interchange).
- 6º) Información que se obtenga de Internet.
- 7º) Transacciones financieras.
- 8º) Software y hardware.
- 9º) Comercio exterior.
- 10º) Comercio interno.
- 11º) Toda documentación que precise movilizarse rápidamente o por el contrario que posea un alto costo de movilización.

#### **Aplicaciones sobre la firma digital**

- 12º) Firma y/o cifrado de correo electrónico, tanto interno como externo.
- 13º) Firma y/o cifrado de documentos (Pericias, dictámenes, planos, software, políticas, procedimientos, normativas, minutas, y otros).
- 14º) Identificación de personas ante sistemas internos en redes locales y abiertas (intranets), sitios Web (sin necesidad de registrar datos).
- 15º) Determinación implícita del perfil de usuario.
- 16º) Identificación de sistemas ante el usuario (¿Cómo sé que es el sistema que dice ser?).
- 17º) Auditoria de transacciones.
- 18º) Seguridad al operar comercialmente (Compra-venta de acciones, transacciones bancarias, operaciones con tarjeta de crédito, y otras).
- 19º) Identificación de los componentes físicos de una red (Computadores, ruteadores, teléfonos celulares, y otros).

#### **Aplicaciones sobre el documento digital firmado digitalmente**

- 20º) Fidelización de documentos digitalizados
- 21º) Cotizaciones de bienes y servicios (tanto el pedido como la cotización y condiciones del proveedor).
- 22º) Resúmenes de cuenta.
- 23º) Recibos de pago.

- 24°) Adjudicaciones.
- 25°) Certificaciones.
- 26°) Factura electrónica.
- 27°) Cheque electrónico.
- 28°) Invitaciones.
- 29°) Promociones.
- 30°) Acreditaciones de puntaje.
- 31°) Remitos de entrega.
- 32°) Ordenes de compra.
- 33°) Solicitudes de adhesión.
- 34°) Contratos.
- 35°) Actas.
- 36°) Planos.
- 37°) Planificaciones.
- 38°) Circulares internas y/o externas.
- 39°) Reservas o turnos para distintas prestaciones (Talleres, médicos, hoteles, pasajes, etc.).
- 40°) Confirmaciones.
- 41°) Autorizaciones de prestaciones médicas.
- 42°) Receta Médica Electrónica.
- 43°) Historia clínica única.
- 44°) Declaraciones juradas.
- 45°) Solicitudes de prestación de servicios.
- 46°) Proyectos.
- 47°) Diseños.

27. Es indudable que otras tantas aplicaciones particulares hacen o pueden hacer uso de las TIC. Sin embargo, por las connotaciones que conlleva la certificación por autoridad

competente especializada del adecuado funcionamiento de las aplicaciones, acorde a las normativas en la materia, las transforma en un tema sumamente delicado. A modo de ejemplo, una aplicación que mayoritariamente contempla el uso de certificados digitales y concordantemente la firma digital es la de correo electrónico y si bien su funcionamiento es razonablemente adecuado a esta situación, adolece de garantías contra defectos que le son imputables, más aún de cara a esta nueva realidad digital/legal.

28. Un aspecto no menor en esta cuestión, es el derivado de la integración, primordialmente cuando las aplicaciones con que se cuenta son paquetes cerrados, nacionales o extranjeros y se desconoce el verdadero tratamiento que se le otorga a la seguridad y principalmente a los datos personales, que ya cuentan con los instrumentos legales para su protección y en donde la implicancia tecnológica y metodológica, aunque existente, conocida y normada, aún no se ha desarrollado adecuadamente.

29. Recordando que en informática y más aún hoy con el enjambre de comunicaciones, software libre, el accionar de los hackers, crackers, y hábiles creadores de virus, gusanos, troyanos, etc., lo aparente no siempre es real, el presagio a partir de aquí es que la consigna es el desafío.

### **LA FIRMA DIGITAL EN LA NORMATIVA ARGENTINA, EL DECRETO 2628/2002 COMO REGLAMENTACIÓN DE LA LEY DE FIRMA DIGITAL**

30. El sistema de firma digital pretende dar una respuesta tecnológica a las transacciones digitales que hoy tienen lugar, brindando seguridad a las mismas, en la medida que los registros electrónicos son fácilmente alterables y, por ende, repudiables, o sea pueden ser desconocidos por alguno de los intervinientes.

31. El propósito de ley 25.506<sup>1</sup>, sancionada en noviembre de 2001 y reglamentada en diciembre de 2002, ha sido reconocer efectos jurídicos a la firma digital, equiparándola con la firma manuscrita.

32. De este modo se ha introducido en nuestro sistema jurídico una adecuación necesaria con el fin de reconocer "modos de firmar", inicialmente no contemplados en las

---

<sup>1</sup> Debido a su importancia en el establecimiento de un marco regulatorio para la infraestructura digital en la Argentina, el texto de la ley se encuentra desarrollado en forma completa en el Anexo "B".

previsiones de nuestro Código Civil. Asimismo, incluye la figura del "documento digital", siendo reconocido como instrumento, cuando es firmado digitalmente.

33. La firma digital se presenta, como una herramienta tecnológica cuyo empleo tiene por finalidad brindar seguridad respecto de la autoría de un documento digital y respecto de la integridad de dicho documento, ofreciendo garantías de que el mismo no ha sido alterado. La finalidad de la firma digital no es ocultar o encriptar información, sino brindar seguridad en el intercambio electrónico de información.

34. Si bien hoy por hoy cualquiera puede solicitar en diversos sitios Web certificados de firma digital para firmar su correo electrónico, dichos certificados tienen un alcance restringido a nivel de e-mails. Hasta tanto no sean emitidos por una autoridad certificante licenciada por el ente licenciante, no tienen más validez que la de un documento firmado electrónicamente, es decir, son tan repudiables como lo son los documentos digitales no firmados digitalmente.

35. La firma digital debe ser susceptible de verificación por terceras partes confiables, de modo tal que resulte factible identificar al firmante y detectar alteraciones en el documento digital, posteriores a su firma. En tal sentido, la Autoridad de Aplicación creada por la ley 25.506 tiene a cargo determinar los procedimientos de firma y verificación, conforme estándares tecnológicos internacionales.

36. Este conjunto de previsiones tecnológicas, normativas e institucionales, conforman lo que se da en llamar la infraestructura de firma digital integrada por el Ente Licenciante, las autoridades certificadoras o certificadores de firma digital, los certificados digitales y a las autoridades de registro.

37. El Poder Ejecutivo Nacional cuenta, desde el año 1998, con una norma, el Decreto 427/98, que autorizó el empleo de firma digital para el perfeccionamiento de actos internos en el ámbito de dicho Poder, siendo Autoridad de Aplicación de dicha norma la por ese entonces Secretaría de la Función Pública. Normas vinculadas a estas temáticas son el Decreto N° 1023/01, referido a compras y contrataciones y la Resolución de la Jefatura de Gabinete de Ministros N° 176/02, que autorizó y puso en funcionamiento una Mesa de Entradas Virtual.

38. Con la reglamentación de la ley 25.506 se completó la regulación normativa a nivel nacional de la firma digital restando ahora que los organismos generados implementen los mecanismos de funcionamiento.

### **EL DECRETO 2628/2002**

39. El Decreto, publicado en el Boletín Oficial del 20 de diciembre de 2002 establece para el ámbito federal lo que se da en llamar una Infraestructura de Firma Digital para ofrecer la autenticación y garantía de integridad para los documentos digitales o electrónicos y constituir de esa forma la base tecnológica que permita otorgarles validez jurídica, regulando el funcionamiento de los certificadores licenciados de manera de garantizar la adecuada prestación de los servicios de certificación.

40. A tal fin crea un Ente Administrador de Firma Digital, encargado de otorgar las licencias a los certificadores, supervisar su actividad y dictar las normas tendientes a asegurar el régimen de libre competencia en el mercado de los prestadores y protección de los usuarios de Firma Digital, supliendo de esa forma una falencia que tenía la Ley 25.506

41. Por su parte, en su articulado regula la conformación de una Comisión Asesora para la Infraestructura de Firma Digital, con un equipo multidisciplinario de especialistas en la materia, con el fin de asesorar y recomendar a la Autoridad de Aplicación estándares tecnológicos, y otros aspectos que hacen al funcionamiento de la mencionada Infraestructura, designando al efecto a la Jefatura de Gabinete de Ministros.

### **LAS FORMAS DE EXPRESAR LA VOLUNTAD DIGITALMENTE**

42. A efectos de reconocer la comprobación de autoría e integridad de un documento, el Decreto discrimina a la firma electrónica de la firma digital basada en certificados digitales emitidos por certificadores licenciados sean estos nacionales o extranjeros (Art. 1 y 3).

43. En caso de tratarse de los certificados digitales emitidos por certificadores licenciados, su utilización permite al emisor estar amparada por las presunciones de autoría e integridad establecidas en los artículos 7° y 8° de la ley citada. Tanto en el caso de la firma electrónica como en el caso de firmas digitales basadas en certificados digitales emitidos por

certificadores no licenciados la carga de la prueba se revierte a quien emite la firma eliminando la presunción de autoría que sólo detenta la firma digital basada en certificados digitales emitidos por un certificador licenciado (Art. 2)

### **LAS COPIAS DE LOS DOCUMENTOS DIGITALES FIRMADOS**

44. El Decreto regula el modo de obtener copias autenticadas a partir de los originales en formato digital firmado digitalmente. Dicha certificación de autenticidad se hará de conformidad a los procedimientos legales, vigentes para el acto de que se trate, identificando el soporte que procede la copia (Art. 5). Este criterio es correcto, a efectos de viabilizar, por ejemplo, la adjunción de contratos celebrados electrónicamente a las demandas que se entablen judicialmente en caso de su incumplimiento.

### **EL ESTÁNDAR TECNOLÓGICO: LA CRIPTOGRAFÍA DE CLAVE ASIMÉTRICA**

45. Dado que la Ley 25.506 - siguiendo un criterio aceptado internacionalmente de normativas "tecnológicamente neutras" - no había definido la tecnología a adoptar para la emisión y reconocimiento de firmas digitales (para evitar su obsolescencia). El Decreto delega en la Jefatura de Gabinete de Ministros como Autoridad de Aplicación la función de establecer los estándares tecnológicos y de seguridad aplicables en consonancia con estándares internacionales así como los procedimientos de firma y verificación en consonancia con dichos estándares, las condiciones mínimas de emisión de certificados digitales (Art. 4) y las denominadas Políticas de Certificación (Art. 29), si bien acepta provisionalmente los Estándares Tecnológicos de Infraestructura de Firma Digital establecidos en la Resolución N° 194/98 de la ex Secretaría de la Función Pública, lo que significa la aceptación expresa de la criptografía de clave asimétrica (Art. 22).

46. El Decreto crea el Ente Administrador de Firma Digital dependiente de la Jefatura de Gabinete de Ministros como órgano técnico, administrativo encargado de otorgar las licencias a los certificadores y de supervisar su actividad bajo un régimen de libre competencia, equilibrio de participación en el mercado de los prestadores y protección de los usuarios (Art. 11).

47. Por último, regula un sistema de auditoria a ser prestado por universidades y organismos científicos y/o tecnológicos nacionales o provinciales, los Colegios y Consejos

profesionales, que acrediten experiencia profesional acorde en la materia (Art. 18) para evaluar los sistemas utilizados por el certificador.

### **EL ARANCELAMIENTO DE LA FIRMA DIGITAL**

48. En el Decreto se faculta al Ente Administrador a arancelar los servicios que preste para cubrir total o parcialmente sus costos. Los recursos propios del Ente Administrador se integrarán con los importes provenientes de los aranceles que se abonen por la provisión de los servicios de certificación digital de firma, de certificación digital de fecha y hora, de almacenamiento seguro de documentos electrónicos, servicios prestados por autoridades de registro o por terceras partes confiables, por servicios de certificación de documentos electrónicos firmados digitalmente u otros servicios o actividades relacionados a la firma digital así como los importes provenientes de los aranceles de homologación de dispositivos de creación y verificación de firmas digitales, los provenientes de los aranceles de certificación de sistemas que utilizan firma digital, de los aranceles de administración del sistema de auditoría y las auditorías que el organismo realice por sí o por terceros (Art. 16).

### **LA OBTENCIÓN DE LA LICENCIA COMO PROVEEDOR DE SERVICIOS DE CERTIFICACIÓN**

49. La norma establece los recaudos para obtener una licencia de provisión de servicios de certificación (Art. 24), que no podrá exceder de 5 años, (si bien admite que pueden ser renovadas indefinidamente), y exige al certificador contar con seguros vigentes acordes con las responsabilidades asumidas (Art. 30) dado que el Estado en su calidad de Ente Administrador de la Infraestructura de Firma Digital no asume responsabilidades por los actos cometidos por los certificadores (Art. 25). Los certificadores están autorizados efectuada a utilizar los servicios de infraestructura tecnológicos prestados por un tercero (Art. 33).

### **LOS CERTIFICADOS DIGITALES EMITIDOS EN EL EXTRANJERO**

50. Se faculta a la Autoridad de Aplicación a "elaborar y firmar acuerdos de reciprocidad con gobiernos de países extranjeros, a fin de otorgar validez, en sus respectivos territorios, a los certificados digitales emitidos por certificadores de ambos países, en tanto se verifique el cumplimiento de las condiciones establecidas por la Ley N° 25.506 y su

reglamentación para los certificados emitidos por certificadores nacionales" (Art. 28).

51. La norma prohíbe a los certificadores licenciados reconocer certificaciones emitidas por certificadores extranjeros correspondientes a personas con domicilio o residencia en la República Argentina y deriva al Ente Administrador de Firma Digital el establecer las relaciones que los certificadores licenciados deberán guardar entre los certificados emitidos en la República Argentina y los certificados reconocidos de certificadores extranjeros (Art. 28).

### **LA AUTORIDAD DE REGISTRO**

52. Los proveedores de servicios de certificación pueden delegar en Autoridades de Registro las funciones de validación de identidad y otros datos de los suscriptores de certificados y de registro de las presentaciones y trámites que les sean formuladas, bajo la responsabilidad del Certificador Licenciado (Art. 35).

53. Dichas Autoridades están igualmente autorizadas para el archivo y la conservación de toda la documentación respaldatoria del proceso de validación de identidad, de acuerdo con los procedimientos establecidos por el certificador licenciado, el cumplimiento de las normas y recaudos establecidos para la protección de datos personales.

54. En las entidades y jurisdicciones pertenecientes a la Administración Pública Nacional, las áreas de recursos humanos cumplirán las funciones de Autoridades de Registro para los agentes y funcionarios de su jurisdicción. En el caso, y si las aplicaciones de que se trate lo requieren, la máxima autoridad del organismo podrá asignar, adicionalmente, a otra unidad las funciones de Autoridad de Registro (Art. 39)

### **LA NORMATIVA REFERIDA A LOS CONTRATOS DE CONSUMO**

55. Los contratos de consumo pueden también ser celebrados por medios electrónicos, entendiéndose por tal aquel que se celebra entre un proveedor y un consumidor a través de la utilización de algún elemento electrónico.

56. La Ley 24.240 define que se entiende por consumidor: "Se consideran consumidores o usuarios, las personal físicas o jurídicas que contratan a título oneroso para su consumo final o beneficio propio o de su grupo familiar o social: a) la adquisición o locación

de cosas muebles; b) la prestación de servicios; c) la adquisición de inmuebles nuevos destinados a vivienda, incluso los lotes de terreno adquiridos con el mismo fin, cuando la oferta sea pública y a personas determinadas.”

57. La mayoría de los países, entre ellos Argentina promueven normativas específicas hacia la protección de los consumidores.

58. Debido a que la contratación por medios electrónicos es llevada a cabo generalmente por partes residentes en distintos Estados, la ley aplicable será distinta a la vigente en el lugar de residencia del consumidor, sea porque está establecido en el contrato o por estar previsto en normas de derecho internacional privado.

59. Las normativas tendientes a la protección de los consumidores no pueden ser dejadas de lado en los contratos celebrados por medios electrónicos, ya que a la situación habitual de inferioridad en que se encuentran los consumidores con relación a los proveedores, se suma la que deriva del distinto grado de conocimiento que tiene cada parte contratante del medio empleado para llevar adelante la contratación.

60. No sería razonable exigirles a los proveedores el conocimiento de la legislación vigente en cada país con el que celebran contratos de consumo, lo cual implicaría elevados costos de transacción y en lugar de proteger al consumidor se estaría generando el efecto contrario, porque los proveedores preferirían no contratar con determinados países.

61. Una solución sería la celebración de acuerdos internacionales en los cuales se establezcan normas mínimas especiales de protección a los consumidores. El objetivo buscado en los acuerdos debe ser intentar disminuir al máximo posible la situación de inferioridad en que se encuentra el consumidor con relación al empresario, lo cual le impediría negociar libremente las cláusulas del contrato.

62. Hay algunos aspectos de la Ley de Defensa al Consumidor vigente en Argentina, que pueden aplicarse a la celebración de los contratos por medios electrónicos:

- 1º) *El deber de información:* La Ley 24.240 prevé en su Art. 4 el deber de brindar, en las relaciones contractuales efectuadas con consumidores, información veraz, detallada, eficaz y suficiente sobre las características esenciales del producto o servicio comercializado. En su Art. 5 estipula que “las cosas y servicios deben ser suministrados o prestados en forma que, utilizados en condiciones previsibles o

normales de uso, no presenten peligro alguno para la salud o integridad física de los consumidores o usuarios. El Art. 6 establece que deberá entregarse un manual en idioma nacional cuando se tratare de cosas o servicios riesgosos. Esta última normativa es de difícil cumplimiento cuando se trata de contratos celebrados por medios electrónicos ya que generalmente los bienes o servicios son producidos, comercializados, distribuidos o prestados en un país distinto a la Argentina. Es necesario que se establezcan tratados internacionales con la normativa aplicable a los contratos de consumo celebrados por medios electrónicos.

- 2°) *Publicidad*: La Ley 24.240 estipula en su Art. 8 que “las precisiones formuladas en la publicidad o en anuncios, prospectos, circulares u otros medios de difusión obligan al oferente y se tienen por incluidas en el contrato con el consumidor.” Esta norma es también aplicable a los contratos celebrados por medios electrónicos.
- 3°) *Oferta a consumidores indeterminados*: La Ley de Defensa al Consumidor estipula en su Art. 7 que “La oferta dirigida a consumidores potenciales indeterminados, obliga a quien la emite durante el tiempo en que se realice, debiendo contener la fecha precisa de comienzo y de finalización, así como sus modalidades, condiciones o limitaciones. La revocación de la oferta hecha pública es eficaz una vez que haya sido difundida por medios similares a los empleados para hacerla conocer.” En un sitio Web, debe tenerse presente que se configuren todos los elementos necesarios que hacen a la oferta, de forma tal que el comprador con la simple aceptación perfeccione el contrato, caso contrario sólo existirá una invitación a ofertar pero no una oferta.
- 4°) *Empleo del idioma nacional*: Este requisito planteado en varios artículos de la Ley de Defensa al Consumidor, si bien no se cumple en la mayoría de los casos de contratos celebrados por Internet, resulta inconveniente su exigencia a los proveedores, ya que es un obstáculo innecesario al desarrollo del comercio electrónico. Esto debido a que si una persona contrató por un sitio Web, leyó las condiciones del mismo redactadas en un idioma distinto al suyo, no sería razonable que invoque esta causa para anular el contrato.
- 5°) *Venta por medios electrónicos*. El Art. 33 de la Ley 24.240 prevé el supuesto de venta a través de medios electrónicos al establecer que “la Venta por correspondencia y otras”, “es aquella en que la propuesta se efectúa por medio postal, telecomunicaciones, electrónico o similar y la respuesta a la misma se realiza por iguales medios.” Es decir que los contratos de consumo por medios electrónicos están contemplados en la legislación argentina.
- 6°) *Garantía y servicio técnico*: “Cuando se comercialicen cosas muebles no consumibles, el consumidor y los sucesivos adquirientes tienen garantía legal por los defectos o vicios de cualquier índole, aunque hayan sido ostensibles o manifiestos al tiempo del contrato, cuando afecten la identidad entre lo ofrecido y lo entregado o su correcto funcionamiento. La garantía legal tendrá vigencia por TRES (3) meses a partir de la entrega, pudiendo las partes convenir un plazo mayor..” . Esto así lo establece el Art. 11 de la Ley 24.240, como también estipula en el Art. 12 que se deberá asegurar un adecuado servicio técnico. En el caso de contratos celebrados por medios electrónicos, a menos que hubiese una sucursal en

el país del consumidor es de difícil aplicación, en todo caso el comprador podría exigir al vendedor una disminución de lo pagado, el envío de una nueva cosa en perfecto estado según lo convenido en la contratación.

7º) *Invalidez de cláusulas abusivas*: el Art. 37 de la Ley 24.240 establece que “sin perjuicio de la validez del contrato, se tendrán por no convenidas: a) las cláusulas que desnaturalicen las obligaciones o limiten la responsabilidad por daños; b) las cláusulas que importen renuncia o restricción de los derechos del consumidor o amplíen los derechos de la otra parte; c) las cláusulas que contengan cualquier precepto que imponga la inversión de la carga de la prueba en perjuicio del consumidor.” El riesgo de la inclusión de estas cláusulas en los contratos de consumo celebrados por medios electrónicos es muy amplio.

### **COROLARIO DEL CAPÍTULO**

63. Lo visto en el capítulo conforma un marco regulatorio de suma importancia para el desarrollo de la infraestructura digital, pero como se verá en el próximo capítulo, el derecho puede dar más en relación al camino hacia una Argentina digital.

## CAPÍTULO II

### **¿Que Provee el Derecho en La Era Digital?**

#### **PROTECCION DE DATOS PERSONALES**

64. El régimen de protección de los datos personales establecido por la Ley 25.326 y reglamentado por el Decreto 1558/2001, también conocido como "Habeas Data", basado en el derecho reconocido por el Art. 43 de la Constitución Nacional, permite que los ciudadanos ejerzan un legítimo poder de disposición y control sobre sus datos personales. A tal fin, los faculta a decidir cuáles de esos datos quieren proporcionar a terceros, sea el Estado o un particular, o qué datos pueden esos terceros recabar, permitiendo asimismo que sepan quién posee sus datos personales y para qué, pudiendo inclusive oponerse a esa posesión o uso.

65. Estos poderes de disposición y control sobre los datos personales, se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Ese derecho a consentir el conocimiento y tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

66. La Ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, públicos o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre. Como se ve, el derecho que se trata de proteger no es sólo el de la intimidad, sino algo con mayor profundidad que en el derecho anglosajón se denomina "privacy" y que se ha castellanizado como "privacidad". Lo que se busca es proteger aspectos de la personalidad que individualmente no tienen mayor trascendencia pero que, al unirse con otros, pueden configurar un perfil determinado de las personas. Ante dicha posibilidad surge el derecho de

sus titulares a exigir que los datos permanezcan en el ámbito de su privacidad.

67. La operacionalización del derecho en este aspecto es la siguiente:

- 1º) Reclamos judiciales y extrajudiciales por infracciones a la ley 25.326 (habeas data y acción de protección de datos personales).
- 2º) Redacción de políticas de privacidad de sitios Web.
- 3º) Consultoría en materia de protección de datos en los sectores de la salud, publicidad, marketing, Internet, informes bancarios y crediticios.
- 4º) Análisis de factibilidad de transferencia internacional de datos personales.
- 5º) Auditoria de bases de datos y adecuación al régimen jurídico argentino.
- 6º) Registro de bases de datos ante la dirección nacional de protección de datos personales.

## **PROPIEDAD INTELECTUAL**

68. Los derechos de propiedad intelectual son los que tiene el autor de un trabajo para autorizar o prohibir su uso. El término utilizado en los países encolumnados en el llamado Derecho Continental (como lo es el Derecho Argentino) es derecho de autor o *droit d'auteur*, mientras los países anglosajones utilizan la expresión *copyright*.

69. En los países de derecho latino, el derecho de autor tiene orientación esencialmente individualista y se restringe a la protección de las expresiones formales que son el resultado de una actividad intelectual de naturaleza creativa, la atribución de la calidad de autor corresponde a la persona física que crea la obra, a quien le reconoce determinados derechos de carácter personal y patrimonial.

70. El derecho de autor reconoce en cabeza del creador de dichas obras intelectuales facultades exclusivas de carácter personal (derecho moral) y de carácter patrimonial (derecho patrimonial) oponibles *erga omnes*.

71. El derecho moral persigue la tutela de la personalidad del autor en relación con su obra. Garantiza intereses intelectuales de carácter extrapatrimonial por una duración ilimitada. Está integrado por el derecho a divulgar la obra o mantenerla reservada en la esfera

de la intimidad, el derecho al reconocimiento de la paternidad intelectual sobre la obra, el derecho al respeto y a la integridad de la obra (la difusión debe ser hecha en la forma en que el autor la creó) y por el derecho al retracto o arrepentimiento por cambio de convicciones (retirar la obra del comercio).

72. El derecho de autor ha sido profundamente impactado por el avance de la informática, ya que la tecnología permite que todo tipo de trabajo intelectual sea modificado, reproducido, distribuido, publicado o transformado sin la autorización de su autor.

73. Si bien es cierto que el derecho común se demoró en aceptar los cambios que ha implicado el rápido avance de la tecnología y la divulgación de Internet en la actualidad existen variados mecanismos para proteger el derecho que los autores tienen sobre sus obras, ya sean de carácter patrimonial o moral.

74. La operacionalización del derecho en este aspecto es la siguiente:

- 1º) Registro de obras de software, bases de datos y obras multimedia.
- 2º) Registro y protección de páginas Web.
- 3º) Tutela de los derechos de autor en Internet.
- 4º) Redacción de contratos de escrow.

### **CORREO ELECTRONICO**

75. Las nuevas tecnologías de la información han modificado la forma en que la gente se comunica, siendo realmente trascendente el fenómeno alcanzado en tal aspecto por la utilización del correo electrónico (Ej.: e-mail).

76. Efectivamente, la utilización de esta nueva forma de comunicación entre las personas ha beneficiado enormemente a las organizaciones, facilitando la comunicación interna entre sus miembros y también con el exterior. De hecho, la implementación del correo electrónico en la empresa ha provocado grandes cambios en la forma de trabajar. No sólo se ha convertido en una nueva y muy importante herramienta de trabajo sino que, además su correcta utilización permite que las empresas puedan reducir costos, implementar nuevas formas de trabajo (Ej.: teletrabajo) y lograr una más eficiente y productiva actividad laboral.

77. Como contrapartida, el uso del correo electrónico en el ámbito laboral, puede suscitar conflictos entre el derecho a la intimidad del trabajador con respecto al contenido de los mensajes por él enviados y el derecho del empresario a ejercer el debido control sobre los bienes de la empresa y controlar que los recursos que pone a disposición del empleado se utilicen única y exclusivamente para desempeñar más eficientemente su labor.

78. Pero no sólo su uso en el ámbito laboral es materia de conflicto. Otra de las cuestiones que suele provocarlos es el envío y recepción masiva de mensajes de correo electrónico publicitarios no solicitados (Ej.: spam).

79. El spam es la técnica de envío indiscriminado de e-mails a miles de usuarios que no pidieron recibirlos e integra el grupo de los llamados abusos en el correo electrónico, pues su práctica trasciende los objetivos habituales del servicio y perjudica a proveedores y usuarios. Si bien la práctica habitual consiste en el envío de correo comercial y publicitario, no son pocos los casos en que se lo utiliza con el fin de paralizar el servicio por saturación de las líneas, del espacio en disco o de la capacidad de procesamiento de un servidor. En la mayoría de los casos el spammer -así se denomina a quienes practican esta actividad- es desconocido y la dirección de correo que aparece en el remitente es falsa, lo que impide identificar una dirección de retorno correcta para responder el mensaje.

80. El Spam ha sido condenado desde los albores de Internet, especialmente por la Netiquette y las RFCs 2505 y 2635, pero también por las asociaciones que nuclean a los proveedores de servicios de Internet y por diversos pronunciamientos judiciales extranjeros. No obstante, son pocas las voces que se alzan a favor de la prohibición total.

81. Varios de los proyectos existentes sobre la materia consideran apropiado el sistema de opt-out que permite a los usuarios solicitar que sus datos sean excluidos de las bases de datos utilizadas por los spammers. Por su parte, las organizaciones protectoras de los usuarios y consumidores prefieren el sistema opt-in, según el cual quien pretenda enviar mensajes comerciales deberá contar con la autorización expresa del destinatario.

82. La operacionalización del derecho en este aspecto es la siguiente:

- 1º) Reclamos por control y monitoreo laboral de mensajes de correo electrónico.
- 2º) Redacción de políticas aceptables de uso del correo electrónico en la empresa.

3º) Reclamos judiciales y extrajudiciales por recepción de mensajes de correo electrónico no solicitados (ej.: spam).

4º) Asesoramiento en creación de bases de datos de direcciones de correo electrónico y envío de mensajes publicitarios on-line.

### **COMERCIO ELECTRONICO**

83. En general, se entiende por comercio electrónico a todo intercambio de datos que se realiza por medios electrónicos, esté o no relacionado estrictamente con la actividad comercial. En un sentido más estricto, debe entenderse por tal a aquel cuya actividad se circunscribe a las transacciones electrónicas desarrolladas a través de los mecanismos que proporcionan tecnologías tales como el correo electrónico, la Web o el EDI.

84. Su principal característica es la de provocar la transformación de los usuales procesos y mecanismos transaccionales basados en papel, en procesos digitales en los que la letra impresa es reemplazada por el lenguaje binario digital, compuesto de cadenas de unos y ceros.

85. Aunque muchos lo supongan, el comercio electrónico no es un fenómeno nuevo. Por el contrario, las primeras formas de comercio electrónico nacieron en la década del '80.

86. De ellas, la más consolidada y aún en vigencia es el EDI (Electronic Data Interchange) que a grandes rasgos consiste en la realización de transacciones comerciales en forma automatizada, mediante el intercambio de todo tipo de instrucciones (órdenes de compra, ventas, pagos, transferencias) entre dos computadoras determinadas. Por lo general, el EDI se desarrolla a través de redes cerradas proporcionadas por un proveedor de servicios determinado, entre integrantes de un mismo sector económico (por ejemplo, entre Bancos) que luego de una etapa de conocimiento y negociación logran establecer protocolos compatibles que les permiten realizar transacciones entre sí.

87. La novedad que trajo Internet a este tipo de formas de realizar transacciones electrónicas es la posibilidad de efectuarlas sin que sea necesario realizar un acuerdo bilateral previo o sin siquiera conocer a la parte con la que se está contratando. De esta manera, a diferencia del EDI, Internet permite personas y/o empresas hasta entonces desconocidas

puedan relacionarse ocasionalmente sin necesidad de contactos previos.

88. Lo antedicho no ha dictado la sentencia de muerte del EDI. Por el contrario, muchas empresas están desarrollando un nuevo navegador de Internet para plataformas EDI que permita conducir el tráfico generado por dicha actividad a través de Internet de una manera más económica, flexible y accesible que el EDI tradicional. Con en esta nueva modalidad llamada Open EDI, las partes implicadas podrán relacionarse directamente a través de Internet sin acuerdos previos.

89. No es ninguna novedad que el comercio electrónico aún genera muchos miedos e incertidumbres entre los operadores económicos, entre los que se destacan la identificación de las partes, el momento de perfeccionamiento del contrato, la validez y eficacia de las transacciones electrónicas, la prueba del contrato, la distribución de responsabilidad entre los contratantes, los problemas de inseguridad y confidencialidad en la información, las formas seguras de pago, la ley aplicable y la jurisdicción competente.

90. Evidentemente, para que el comercio electrónico pueda desarrollarse se necesita que todos los operadores involucrados en esta nueva forma de hacer negocios (empresarios, consumidores, intermediarios, proveedores de servicios, etc.) tengan confianza en que sus transacciones no serán interceptadas ni modificadas, que las partes que contratantes son las que dicen ser, que los mecanismos de transacción y pago son seguros y que, en caso de conflicto, estarán amparados por normas y procedimientos eficaces a fin de salvaguardar sus derechos.

91. Existen en la actualidad muchas de formas de lograr que esos objetivos se cumplan y es por ello que el comercio electrónico ha dejado de ser una utopía para transformarse en una realidad.

92. Entre ellas, la más reciente es el reconocimiento jurídico que la legislación de varios países del mundo, entre ellos Argentina, le ha otorgado a la firma digital.

93. Es común la confusión entre el significado de la firma digital con el de la firma electrónica.

94. La firma electrónica es aquella que un firmante coloca en forma digital sobre unos datos, añadiéndola o asociándola lógicamente a los mismos, y la utiliza para indicar su

aprobación respecto del contenido de esos datos. En líneas generales, cumple los siguientes requisitos: a) vinculada únicamente al firmante, b) capaz de identificar al firmante, c) creado utilizando un medio técnico que está bajo el control del firmante, y d) vinculada a los datos a los que se refiere.

95. Una clase particular de firma electrónica que permite ofrecer mayor seguridad a los usuarios es la firma digital asimétrica de clave pública. Este tipo de firmas consiste en un criptosistema basado en el uso de un par de claves asociadas: una clave privada que se mantiene en poder de su titular y una clave pública que se distribuye libremente para que sea conocida por cualquier persona.

96. Básicamente el procedimiento de la firma digital de clave asimétrica es el siguiente: 1) El emisor de un mensaje lo cifra digitalmente utilizando su clave privada. 2) El receptor del mensaje puede descifrarlo utilizando la clave pública del emisor.

97. Como la aplicación de criptografía asimétrica sobre la totalidad del mensaje es muy costosa, en los mensajes de gran extensión, suele aplicarse sobre el mismo un algoritmo de resumen que transforma una secuencia de bits en uno menor, llamada función hash. Al aplicar esta función se obtiene un resumen del mensaje denominado huella digital, cuyas características principales son su irreversibilidad (a partir del hash no puede obtenerse el mensaje completo) y la imposibilidad de obtener un segundo mensaje que produzca el mismo resumen, de forma que cualquier cambio en el mensaje produciría un hash diferente.

98. Una vez aplicada la función hash al mensaje principal, el resumen resultante es cifrado con la clave privada del firmante y es enviado junto al mensaje original, de forma tal que el receptor, para comprobar que el mensaje ha sido firmado por el emisor, debe realizar dos operaciones: descifrar el hash aplicando la clave pública del emisor y aplicar la función hash sobre el mensaje completo obtenido. Si el hash recibido y descifrado y el hash obtenido coinciden, habrá verificado que el mensaje ha sido enviado por quien dijo haberlo hecho y que su contenido no ha sufrido alteraciones.

99. Estos sistemas de criptografía asimétrica permiten enviar mensajes confidenciales, proporcionando autenticidad, integridad y no repudio por parte del destinatario y, de acuerdo al estado del arte actual, alcanzan el nivel de seguridad necesario para poder asimilarlas a la firma escrita en papel.

100. Si bien hasta el momento la mayoría de las normas dictadas sobre la materia, incluyendo la Ley Argentina, se basan en este tipo de firma, considero que el mejor criterio legislativo debe adoptar una posición abierta que permita el desarrollo de nuevas técnicas y no se limite a entronizar a este sistema en desmedro de mejores técnicas futuras.

101. La operacionalización del derecho en este aspecto es la siguiente:

- 1º) Asesoramiento jurídico en negocios B2C y B2B.
- 2º) Análisis de legalidad y redacción de términos de uso de páginas Web.
- 3º) Auditoria de sitios Web.
- 4º) Consultaría en comercio electrónico directo e indirecto.
- 5º) Redacción de acuerdos de intercambio electrónico de datos.
- 6º) Asesoramiento en implantación de firma electrónica.

## **CONTRATOS**

102. La operacionalización del derecho en este aspecto es la siguiente:

- 1º) Contratos de acceso a Internet.
- 2º) Contratos de diseño y desarrollo de sitios Web.
- 3º) Contratos de alojamiento de sitios Web (contratos de hosting).
- 4º) Contratos de patrocinio comercial y publicidad.
- 5º) Acuerdos de intercambio de links y alianzas estratégicas.
- 6º) Acuerdos de confidencialidad y secreto empresarial.

## **DEFENSA AL CONSUMIDOR**

103. La operacionalización del derecho en este aspecto es la siguiente:

- 1º) Reclamos por infracciones a la ley de defensa al consumidor.
- 2º) Venta a distancia.

3º) Publicidad engañosa.

### **LEALTAD COMERCIAL**

104. La operacionalización del derecho en este aspecto es la siguiente:

1º) Reclamos por infracciones cometidas por uso desleal de marcas, nombres y denominaciones comerciales en sitios Web, links y metatags.

### **NOMBRES DE DOMINIO**

105. Los nombres de dominio son las letras que identifican a un sitio Web. Al leer una dirección de izquierda a derecha se empieza desde lo particular hacia lo general, es decir, siguiendo una jerarquía de términos o niveles con un mayor o menor poder de identificación.

106. El comando "http://" describe el protocolo de comunicación propio del sistema WWW, señalando que se trata de una información presentada en formato hipertextual. El resto de la dirección es el nombre de dominio. En él se distinguen, separados del protocolo de comunicación y entre sí por un punto: la abreviatura genérica que constituye el nombre de dominio de primer nivel (Top Level Domain o TLD), y la combinación de letras correspondiente a la página Web, conocida como dominio de segundo nivel (Second Level Domain o SLD).

107. Desde los comienzos de Internet el sistema estuvo controlado por IANA (autoridad asignada para la numeración de Internet), una organización semioficial nacida en la Universidad del Sur de California. Con la explosión de Internet IANA se vio desbordada y el Gobierno de Estados Unidos decidió conceder, a partir de un acuerdo con la Fundación Nacional para las Ciencias, el monopolio absoluto sobre la gestión y mantenimiento de los servidores de los dominios ".com", ".org" y ".net" y de WHOIS a la empresa NSI (Network Solutions Inc.) por un período de seis años.

108. Desde un principio han existido los siguientes 7 tipos de dominio de primer nivel: ".edu"; ".org"; ".com"; ".mil"; ".gov" y ".net". En la actualidad, el número de dominios de primer nivel se ha ampliado a 14, incluyendo los nuevos TLDs: ".info"; ".aero"; ".coop";

".museum"; ".biz"; ".name" y ".pro".

109. Además de todos estas abreviaturas genéricas existen otras correspondientes a dominios de primer nivel de carácter geográfico o nacional conocidos como "country code Top Level Domain" (ccTLD) o "national Top Level Domain" (nTLD) que se corresponden con los distintos países desde los que puede accederse a la Red.

110. Cada vez que se publica un sitio en la Web se debe registrar en un organismo que administra el funcionamiento de Internet.

111. En la República Argentina, el organismo encargado de registrar los nombres de dominio con la indentificación de país (.ar), es el Network Information Center dependiente del Ministerio de Relaciones Exteriores, Comercio Internacional y Culto (NIC-ARGENTINA). Su rol principal consiste en administrar el Dominio de Nivel Superior Argentina, sus servicios de registro, la promoción del desarrollo de la infraestructura y tecnología Internet, y la cooperación mutua con otras entidades del Estado.

112. NIC-ARGENTINA efectúa el registro de nuevas denominaciones bajo los subdominios "com.ar", "org.ar", "gov.ar", "mil.ar", "net.ar" e "int.ar".

113. A nivel mundial, con el objeto de reestructurar la forma en que se registran los nombres de dominio y solucionar problemas tales como la apropiación ilegal de nombres de dominio abusando de marcas registradas de terceros, se aprobó en Ginebra el "Acuerdo de Principios" que propone que los nombres de dominio sean de propiedad pública y que se establezca un mecanismo administrativo para evitar la apropiación indebida de nombres.

114. En Argentina, las reglas impuestas por NIC-Ar tampoco han podido evitar el registro masivo y malintencionado de nombres de dominio por personas que, en muchos casos, no ostentan derecho alguno sobre la denominación registrada, pero no existe aún un mecanismo administrativo de solución de controversias.

115. La operacionalización del derecho en este aspecto es la siguiente:

- 1º) Registro y gestión de nombres de dominio en organismos nacionales e internacionales.
- 2º) Reclamos judiciales y extrajudiciales por usurpación de nombres de dominio.

- 3º) Recuperación de nombres de dominio en argentina y el exterior (ompi).
- 4º) Transferencia y cesión de nombres de dominio.
- 5º) Registro de marcas y nombres comerciales.

### **RESPONSABILIDAD CIVIL**

116. La operacionalización del derecho en este aspecto es la siguiente:

- 1º) Responsabilidad civil contractual y extracontractual de los proveedores de servicios de Internet.
- 2º) Reclamos por daños y perjuicios producidos por medios electrónicos y digitales.
- 3º) Consultaría en contenidos nocivos e ilícitos en Internet.
- 4º) Reclamos por daños al honor, imagen e intimidad en Internet.

### **COROLARIO DEL CAPÍTULO**

117. En este capítulo hemos desarrollado el marco legal principal existente, y hemos visto la operacionalización del derecho en relación a las TIC. En el próximo capítulo se hará una síntesis del marco legal existente completo.

### **CAPÍTULO III**

#### **Marco Legislativo y Proyectos**

##### **LEGISLACIÓN Y PROYECTOS**

118. El marco legislativo y proyectos existentes nos ofrecen una idea general del desarrollo del derecho en relación a las TIC en la Argentina, el marco legal se divide en:

- 1º) Comercio Electrónico.
- 2º) Contratos.
- 3º) Correo Electrónico.
- 4º) Delitos.
- 5º) Nombres de Dominio.
- 6º) Documento Electrónico.
- 7º) Firma Digital.
- 8º) Internet.
- 9º) Protección de Datos Personales.
- 10º) Problema del Año 2000.
- 11º) Propiedad Intelectual.

119. El desarrollo de estos contenidos es el siguiente:

##### **COMERCIO ELECTRONICO**

- 1º) Anteproyecto de Ley Formato Digital de los Actos Jurídicos. Comercio Electrónico (Presentado en el Congreso en el mes de Agosto de 2000).
- 2º) Resolución 412/99 del Ministerio de Economía y Obras y Servicios Públicos. Recomendaciones del Grupo de Trabajo sobre Comercio Electrónico y Comercio Exterior.

## **CONTRATOS**

3º) Ley 24.240 de Defensa al Consumidor.

## **CORREO ELECTRONICO**

4º) Anteproyecto de Ley de Regulación de las Comunicaciones Comerciales Publicitarias por Correo Electrónico (SPAM).

5º) Anteproyecto de Ley de Protección Jurídica del Correo Electrónico.

## **DELITOS**

6º) Anteproyecto de Ley de Delitos Informáticos.

7º) Ley 863 de la Legislatura de la Ciudad Autónoma de Buenos Aires sobre Protección del Acceso de los Menores a Páginas Web con Contenido Pornográfico.

8º) Proyecto de Ley del Defensor del Pueblo de la Nación sobre pornografía infantil en Internet.

## **NOMBRES DE DOMINIO**

9º) Resolución 2226/2000 del Ministerio de Relaciones Exteriores, Comercio Internacional y Culto relativa a la Registración de Nombres de Dominio en Internet en la República Argentina.

## **DOCUMENTO ELECTRONICO**

10º) Ley 24.624, modificatoria de la Ley 11.672, que considera con pleno valor probatorio a la documentación de la Administración Pública Nacional archivada en soportes electrónicos.

## **FIRMA DIGITAL**

11º) Resolución 45/97 de la Secretaría de la Función Pública sobre firma digital.

12º) Decreto 555/97 sobre firma digital.

13º) Resolución 194/98 de la Secretaría de la Función Pública que aprueba los estándares aplicables a la "Infraestructura de Firma Digital para el Sector Público Nacional".

14°) Decreto 427/98 que dispuso promover el uso de la firma digital en toda la Administración Pública Nacional, otorgándole similares efectos que la firma manuscrita para los actos internos de administración.

15°) Ley 25.506 de Firma Digital.

16°) Anteproyecto de Decreto Reglamentario de la Ley N° 25.506 de Firma Digital.

17°) Decreto 2.628/02 que reglamenta la Ley N° 25.506 de Firma Digital.

18°) Decreto 283/2003 que autoriza, con carácter transitorio, a la Oficina Nacional de Tecnologías Informáticas a proveer certificados digitales para su utilización en aquellos circuitos de la Administración Pública Nacional que requieran firma digital.

### **INTERNET**

19°) Decreto 554/97 que declara de interés nacional al acceso a Internet.

20°) Decreto 735/97 que crea la Comisión de Conexión con Internet.

21°) Decreto 1279/97 que declara comprendida la garantía constitucional de libertad de expresión para Internet..

22°) Resolución 2132/97 que adopta el procedimiento de Audiencia Pública para la presentación de inquietudes sobre aspectos relacionados con Internet.

23°) Decreto 1018/98 que aprobó el programa "argentin@internet todos" destinado a masificar la utilización de equipamiento multimedia y el acceso a Internet.

24°) Resolución 1235/98 que determina la inscripción que deben incluir las facturas emitidas por los Internet Providers.

25°) Decreto 1293/98 que declara de interés nacional al Proyecto Internet 2.

26°) Decreto 1335/99 que declara de interés nacional al Proyecto "Una dirección de correo electrónico para cada argentino".

### **PROTECCION DE DATOS PERSONALES**

27°) Ley 24.766 de confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos.

28°) Constitución Nacional modificada en 1994. Art. 43.

29°) Ley 25.326 de Protección de los Datos Personales.

30°) Decreto 1.558/2001 que reglamenta la Ley de Protección de los Datos Personales.

31°) Disposición N° 1/2003. Apruébanse la "Clasificación de Infracciones" y la "Graduación de las Sanciones" a aplicar ante las faltas que se comprueben.

### **PROBLEMA DEL AÑO 2000**

32°) Resolución 125/97 de la Secretaría de la Función Pública que crea la Unidad Ejecutora 2000 a fin de controlar el impacto del problema del año 2000 en la administración pública.

33°) Resolución 173/99 de la Secretaría de Industria que obliga a quienes comercialicen equipos de computación o programas que dependan de una variable temporal que incluya el dato "año" a colocar una identificación sobre el carácter compatible o no con el año 2000.

34°) Resolución 512/99 de la Comisión Nacional de Telecomunicaciones que intima a los prestadores de servicios de telecomunicaciones y correo postales a presentar informes sobre la actividad del año 2000.

35°) Comunicaciones "A" 2564, 1654, 2693 y 2959 del Banco Central de la República Argentina a las Entidades Financieras tendientes a lograr la adecuación de los sistemas informáticos para su uso a partir del año 2000.

36°) Circular 3708 de la Superintendencia de Seguros de la Nación solicitando información a las entidades aseguradoras referida a las acciones tomadas previendo el problema del año 2000 y alertando sobre sus responsabilidades.

### **PROPIEDAD INTELECTUAL**

37°) Decreto 165/94 de protección al software.

38°) Ley 24.425 de ratificación de los Acuerdos Trip's.

39°) Ley 25.036, modificatoria de la Ley 11.723 de propiedad intelectual, que incluye dentro de las obras intelectuales protegidas a los programas de computación.

### **DECRETO 724/2006**

120. Es oportuno desarrollar brevemente el texto del Decreto 724/2006<sup>2</sup> por cuanto se configura como un paso más hacia una Argentina con un mejor marco jurídico que sustente el desarrollo de los negocios digitales.

---

<sup>2</sup> El texto completo del Decreto 724/2006 se encuentra desarrollado en el Anexo "B".

121. El Presidente de la Nación ha firmado el 8 de junio del corriente año este decreto que modifica el Decreto N° 2628/02, reglamentario de la Ley 25.506 de Firma Digital. La nueva norma hace opcional la exigencia de constituir seguros, regula la aceptación por parte de terceros usuarios de los documentos firmados digitalmente, habilita a las entidades y jurisdicciones de la Administración Pública Nacional para actuar como certificadores licenciados y para emitir certificados para agentes, funcionarios y particulares y establece condiciones para la firma digital en aplicaciones en que los organismos públicos interactúan con la comunidad.

122. Este Decreto constituye un nuevo avance hacia la consolidación de la firma digital en nuestro país. A partir de esta reglamentación, se espera la próxima aprobación de las normas referidas al proceso de licenciamiento de certificadores, con lo que la Infraestructura de Firma Digital prevista en la Ley 25.506 se encontrará plenamente operativa.

### **COROLARIO DEL CAPÍTULO**

123. Una recorrida del marco legal existente deja una idea de que en la República Argentina, el derecho sigue de lejos la ola tecnológica y de ningún modo es un derecho proactivo a nivel nacional, basándose en tecnologías, experiencias o desarrollo legal foráneo. Más aún, lo que surge de una recorrida general del marco legal es que no existe un efectivo sustento para el desarrollo de los negocios digitales, que ocuparán la primera mitad de este siglo.

## CAPÍTULO IV

### **Conclusiones**

*"La próxima revolución ya está entre nosotros. No es una revolución en tecnología, equipamiento, técnicas, software o velocidad. Es una revolución en los conceptos."*

**Peter Drucker, 1998**

### ARGENTINA EN LA ERA DE LOS NEGOCIOS ELECTRÓNICOS

124. En los artículos periodísticos transcritos en el Anexo "A" y analizados para este trabajo se encuentran algunas claves que permiten vislumbrar cual sería el cauce a seguir para introducir a la República Argentina en la Era de la Información.

125. En el primer artículo se menciona que la Argentina ingresa al Siglo XXI sin una iniciativa o plan coherente, se señala que la participación del país requiere un cambio cultural en sus dirigentes sobre la comprensión y alcance de la naturaleza del fenómeno. Vaticina un crecimiento del 33% y un aumento en la transparencia del Estado o la facilidad para los negocios si se desarrollan las TIC necesarias y consigna un rol fundamental del Estado para hacerlo.

126. En el segundo artículo menciona que la Argentina no tiene futuro si no exporta tecnologías y que el desafío está en promover una verdadera revolución de las TIC. Agrega, a la falta de cultura en el nivel político, la falta de una estrategia global para fomentar inversiones y orientar a los ciudadanos y reafirma el liderazgo necesario del gobierno para lograr los cambios.

127. En el tercer artículo se analiza el caso de Nueva Zelanda y su similitud con el de Argentina, países ambos con una economía agrícola ganadera, productores de commodities que se devaluaron diez veces en un siglo, junto al deterioro de los términos del intercambio, fallando ambos Estados en la transición de sus economías tradicionales hacia una economía de la información.

128. Estos artículos coinciden en un eje que corta transversalmente todo el desarrollo futuro del país, la necesidad de un proyecto, una iniciativa nacional en el área que debe ser liderada desde arriba, con una alta participación corporativa.

129. Las nuevas tecnologías de la información y de las comunicaciones (TIC) impactan fuertemente sobre la economía:

- 1º) Acelerando e incrementando los negocios entre empresas.
- 2º) Mejorando a las empresas, haciéndolas más eficientes para producir mejor a menores costos.
- 3º) Haciendo ganar eficiencia al Estado, brindando mejores servicios con menor peso para la economía del país.
- 4º) Mejorando la competitividad de la Argentina.

130. La instalación de las TIC en la Argentina no se ha producido en la medida deseada, en grado incluso inferior al de países menos favorecidos. Ello se debe fundamentalmente a la falta de iniciativa y liderazgo en el Gobierno, a un problema cultural, desconocimiento del tema de nuestra clase dirigente y, en cierta forma, una costumbre o aceptación de que todo llega a la Argentina con cierto retraso.

### **COORDINACIÓN NORMATIVA INTERNA E INTERNACIONAL (MERCOSUR)**

131. Una de las tareas más importantes es la iniciativa normativa a nivel interno (nacional e interprovincial), y externo, con tratados internacionales. Particularmente importante es la coordinación en el ámbito del MERCOSUR.

132. Un costado oscuro de las tecnologías es que pueden desnudar la privacidad. El Gobierno tiene un importante rol a cumplir en este aspecto.

### **LA REINVENCIÓN DE LAS EMPRESAS**

133. El impacto de las TIC en las empresas se produce de una doble forma: porque incrementa y acelera los negocios entre las empresas y entre ellas y los consumidores.

134. Las TIC e INTERNET están cambiando las empresas de arriba a abajo y de adentro hacia afuera. Les está ayudando a bajar drásticamente sus costos redefiniendo sus

relaciones de negocios. Y como tanto los compradores como los vendedores están reduciendo sus costos e incrementando su eficiencia invirtiendo en su capacidad de hacer negocios en INTERNET, en su propio interés es útil convencer a más empresas con las que hacen negocios para imitarlos, generando un círculo virtuoso.

135. Con los e-business los beneficios se advierten no solamente acelerando y automatizando los procesos internos sino también por la habilidad de diseminar tal eficiencia hacia sus proveedores, socios estratégicos y clientes. La habilidad para colaborar con otros para convertirse en una ventaja tan grande como la habilidad en posicionarse tecnológicamente.

136. En síntesis, las TIC provocarán un fuerte impacto en la economía con su difusión y utilización en las empresas.

137. El principal impacto que producirá en las empresas las TIC tendrá valor por su propia incorporación y la utilización que de ellas se le da en las empresas, así como también por los cambios que se producirá en las mismas empresas, y en la estructura de la forma de hacer negocios.

138. En la Argentina todavía no se advierte ningún movimiento decidido en esta dirección; por el contrario, los ejemplos que existen parecen ser más la excepción que confirma la regla.

### **PERSPECTIVAS DEL COMERCIO ELECTRÓNICO**

139. El advenimiento del comercio electrónico (en su acepción restringida) es hoy una realidad insoslayable. Al igual que en muchas otras áreas, las TIC están transformando el comercio de tal manera que resulta indispensable comenzar a imaginar los distintos campos en que estos cambios influyen e influirán en un futuro muy próximo. Pero por el momento, este impacto será relativo, al menos en relación con los negocios Business to Business.

140. América Latina tiene dos particularidades en su población: a) alta movilidad. Mucha población de América se encuentra fuera de América Latina (fundamentalmente en los EE.UU.), siendo a su vez un grupo económicamente activo, que envía divisas a América Latina; b) no existe una equitativa distribución de la riqueza, ni un desarrollo de la cultura de

la "Tarjeta de Crédito". Por lo que es frecuente que aquellos que pudieran volverse en un público potencial del Comercio Electrónico no pudieran obtener los bienes y/o servicios ofrecidos al no contar con Tarjetas de Crédito.

141. El tema de la seguridad es el de los más importantes dentro de un plan global para el ingreso de los países en la economía digital. La naturaleza de los temas involucrados exige la acción conjunta del sector privado y el gobierno.

142. El desarrollo del comercio electrónico requiere, asimismo, del aggiornamiento legislativo, de forma tal que se reconozca la validez jurídica del soporte electrónico y de mecanismos de identificación o autenticación. Pero ello debe ser realizado a la luz de los principios, cultura y tradiciones que iluminan las legislaciones de los países de derecho civil, de forma tal que los actos realizados por medio y con la utilización de las nuevas soluciones estén rodeadas de la seguridad jurídica indispensable para el correcto funcionamiento de la sociedad.

143. Se encuentran algunas iniciativas bastante coherentes en materia de comercio electrónico, sin perjuicio de que insistimos en que si formaran parte de un plan nacional tendrían mucha más fuerza y resaltarían la verdadera importancia que este tipo de esfuerzos presentan. (Ministerio de Economía a través del Grupo de Trabajo sobre Comercio Electrónico y Comercio Exterior y la participación de nuestro país en la COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL, sobre todo en lo referido a la Ley Modelo sobre Comercio Electrónico, Secretaría de la Función Pública y la Comisión Nacional de Valores.

### **EL ROL DEL GOBIERNO: LIDERAR EL CAMBIO**

144. El Gobierno tiene un rol muy importante a cumplir en esta empresa, y en la Argentina no lo ha asumido. En la mayoría de los países desarrollados, cualquiera fuera el signo económico de la administración que lo dirigía, esto se ha hecho, pues es un campo donde su tarea es fundamental en diferentes áreas:

1º) Coordinación

2º) Liderazgo

- 3°) Neutralidad
- 4°) Infraestructura
- 5°) Iniciativas
- 6°) Legislación
- 7°) Cambio cultural
- 8°) Protección de la privacidad
- 9°) Asumir la utilización de las TIC en la misma administración pública.

145. La Argentina debe desarrollar una iniciativa propia, ya sea

- 1°) Adoptando alguno de los modelos existentes (IS en la Unión Europea, NII en los EEUU, o la de otros países)
- 2°) Haciendo una combinación entre ellas.
- 3°) Desarrollando una iniciativa propia.
- 4°) Este trabajo puede iniciarse convocando a una reunión de expertos e, inclusive, contratando a expertos extranjeros.

### **PROPULSAR A LAS TIC**

146. Debe elaborarse una estrategia para la divulgación de las TIC y debe sustentarse en la actividad privada. Sin perjuicio de ello el Estado Nacional tiene un importante rol a cumplir, debiéndose concentrar en la estrategia antes que en la ejecución, y, en algunos casos, asumiendo el liderazgo. La sola mención de las ventajas 'sociales' de estas tecnologías (en salud, educación, eficiencia del gobierno) no será suficiente para que los recursos privados se vuelquen al desarrollo de la red: debe educarse a los directivos de las organizaciones en los fenómenos de la Revolución Digital y sus expresiones, especialmente INTERNET.

147. La estrategia debe enfatizar en el crecimiento de la competitividad del país, debe fomentar la actividad privada sobre las TIC, debe proveer a la elaboración de planes de acción para acceder a financiación internacional de fomento de nuestra competitividad. En este sentido el Gobierno debe dictar medidas de promoción eliminando impuestos sobre todo lo relacionado con INTERNET, y las transacciones que la utilicen, pensando que lo que pierda allí será sobradamente compensado con lo que ganará el país.

148. El Gobierno tiene que conformar el trípode sobre el cual avanzan los países más adelantados de la tierra: (a) Gobierno (Poder Ejecutivo y Parlamento), (b) Academias (universidades y centros de investigación) y (c) empresas. Esta estructura no se encuentra integrada hoy en la Argentina y el marco legal requerirá mucho desarrollo.

149. Si la revolución no es conducida de arriba hacia abajo, si no es acompañada desde el derecho, por más ancha que sea la banda, por más óptica que sea la fibra, por más alta o baja que sea la trayectoria del satélite, por más credibilidad que tenga la autoridad certificante que firma el certificado que acompaño con mi firma digital, si los verdaderos revolucionarios, hombres y mujeres que con su imaginación e inventiva darán lugar a los nuevos contenidos, no comprenden lo que se les dice, la tecnología seguirá funcionando en los laboratorios.

## *Glosario de Términos*

**Firma Electrónica:** Conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizados por el signatario como su medio de identificación, que carezca de algunos de los requisitos legales para ser considerada firma digital.

**Firma digital:** Resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control, susceptible de verificación identificar al firmante y detectar cualquier alteración del documento digital, posterior a su firma.

**Documento Digital o Electrónico:** Representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento archivo.

**Certificado Digital:** Documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.

**Certificador Licenciado:** Persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante.

**Política de Certificación:** Conjunto de criterios que indican la aplicabilidad de un certificado.

**Clave criptográfica privada:** En un criptosistema asimétrico es aquella que se utiliza para firmar digitalmente.

**Clave criptográfica pública:** En un criptosistema asimétrico es aquella que se utiliza para verificar una firma digital.

**Integridad:** Condición que permite verificar que una información no ha sido alterada por medios desconocidos o no autorizados.

**Criptosistema asimétrico:** Algoritmo que utiliza un par de claves, una clave privada para firmar digitalmente y su correspondiente clave pública para verificar dicha firma digital

## *Bibliografía*

### **LIBROS**

Eco, Humberto - Como se Hace una Tesis, ed. Gedisa, España, 1992.

Horacio M. Lynch -Argentina Digital - El impacto de la Revolución Digital en la Argentina, ed. Cenit, Buenos Aires, 1999

### **ARTÍCULOS**

Ing. Daniel Edgardo Cortés - Derecho y Nuevas Tecnologías, Aplicaciones con firma digital.

Horacio M. Lynch - El documento y la firma digital en el Derecho Argentino, Comentario a la Ley 25,506 de firma y documento digital, sobre la base de una colaboración publicada por la revista ANALES DE LEGISLACIÓN ARGENTINA, ed. LA LEY (Boletín Informativo, año 2001, No. 34)

Horacio M. Lynch – El Derecho y las Nuevas Tecnologías de la Información y de las Comunicaciones, Jornadas de la Comunicación – Facultad de Ciencias de la Información Universidad Austral, en la sede de Juan de Garay, Buenos Aires, Argentina, 2001.

Horacio R. Granero - Comentarios al Decreto 2628/2002 (Reglamentación de la Ley de Firma Digital).

### **SITIOS WEB**

Introducción a Internet y sus relaciones con el derecho, Argentina Digital III: el diseño del marco legal, Investigación #12/00.

<http://www.it-cenit.org.ar/Publicac/ArgentinaDigital/ArgDig3.htm> - Fecha 15 Agosto 2006.

## ARTÍCULOS PERIODÍSTICOS

150. En el presente anexo se detallan algunos ejemplos publicados en periódicos nacionales acerca de la infraestructura digital en la Argentina..

### **Editorial I**

## **La Argentina y la revolución digital**

UN reciente artículo del columnista Andrés Oppenheimer, publicado en *La Nación*, llama la atención sobre un hecho insospechado: el éxito que ha alcanzado la República Dominicana en sus esfuerzos por colocarse en situación de competir en la economía informática, que en el futuro, seguramente, será de fundamental importancia para el crecimiento de cualquier nación.

Un país centroamericano que hasta hace poco no parecía tener demasiadas posibilidades de insertarse en la economía mundial -y cuyos recursos parecían limitarse a la explotación del turismo- está hoy en vías de convertirse en un importante centro de procesamiento de datos y programación de Internet.

El pilar del proyecto dominicano es la construcción -en las afueras de la capital del país- de un parque cibernético de alta tecnología que está atrayendo cada vez con más fuerza a las compañías extranjeras interesadas en desarrollar, con mano de obra barata, instalaciones de software, servicios de diseño y contenido de Internet y operaciones de banco de datos.

Ante esta información, parece inevitable reflexionar sobre la situación en que se encuentra la Argentina frente a los requerimientos de la llamada era digital o era de la información. Nuestro país se dispone a ingresar en el siglo XXI sin una iniciativa o plan coherente para afrontar las exigencias de la economía digital, imprescindible para toda sociedad que aspire a un crecimiento genuino en el competitivo mundo que se avecina.

Es interesante conocer las conclusiones de un informe producido recientemente por el *Centro de Investigaciones en Information Technology* (Cenit), institución creada en 1997 para analizar el impacto de las nuevas tecnologías de la información y de las comunicaciones sobre la economía, la educación, el derecho, los medios de prensa y otros aspectos culturales y técnicos de la vida argentina. El informe está contenido, en todos sus detalles, en el libro "Argentina digital", de Horacio M. Lynch y Mauricio Devoto, directores del Cenit, que fue editado en noviembre de este año.

La participación de nuestro país en la nueva era de la información -señalan los autores- requiere de un cambio cultural. Es indispensable que los niveles directivos de la actividad nacional (gobierno, empresarios, dirigentes de las instituciones educativas y de las organizaciones no gubernamentales) comprendan la naturaleza y el alcance del fenómeno al que hay que hacer frente.

Para que la Argentina se coloque en situación de entrar de lleno en la digitalización - puntualiza el informe del Cenit- no hacen falta grandes inversiones: lo que se necesita es que la dirigencia se sienta a pensar y que el tema se instale en la sociedad como debate. El resultado último de esa toma de conciencia deberá ser la elaboración de un plan de acción nacional que fije los pasos fundamentales para acercar nuestro país a la economía digital.

El impacto de las nuevas tecnologías de la información y de las comunicaciones sobre la economía promete ser altamente benéfico. El uso intensivo de los recursos informáticos acelera e incrementa los negocios entre empresas, mejora la competitividad del país, contribuye a que los empresarios nacionales produzcan mejor y a menores costos y permite que el Estado gane en eficiencia y, sobre todo, en transparencia y confiabilidad moral.

Aunque es casi imposible medir con precisión el beneficio que la digitalización podría traer a nuestra economía, se estima que el crecimiento sería de alrededor del 33 por ciento, con las consiguientes consecuencias sobre el producto bruto interno (PBI).

Una tarea que no podrá ser eludida es la creación de un marco legislativo que otorgue validez jurídica a las transacciones comerciales realizadas mediante soportes electrónicos, y que establezca los correspondientes mecanismos de identificación o autenticación. Todo ello deberá hacerse, por supuesto, a la luz de los principios, las tradiciones y la cultura propios del derecho civil, de modo que los negocios digitales estén rodeados de la seguridad jurídica indispensable para el correcto funcionamiento del sistema.

El gobierno tiene un rol fundamental en esta empresa: su misión es liderar el cambio, dictar medidas que promuevan la economía electrónica, asegurar una activa presencia argentina en los foros internacionales, proteger la privacidad de los usuarios de las redes electrónicas, coordinar las normativas correspondientes en el ámbito del Mercosur y, fundamentalmente, diseñar y ejecutar propuestas educativas acordes con las necesidades de una sociedad de la información.

Las autoridades nacionales -y, globalmente, la dirigencia política y económica- deberían prestar especial atención a las advertencias sobre la necesidad de preparar y estimular el ingreso pleno de la sociedad argentina en la etapa de la economía digital. Más que un problema de recursos, es un problema de naturaleza cultural y, complementariamente, de decisión política.

Miércoles 23 de febrero de 2000

INFORMATICA PAPEL

COLUMNA DE OPINION DEL SUPLEMENTO INFORMATICA DE CLARIN DEL 23/2/00

## Hacia una Argentina digital

HORACIO M. LYNCH Y MAURICIO DEVOTO

En opinión de muchos especialistas respetados en el mundo, la Argentina no tiene futuro si no exporta. Pero exportar en este nuevo siglo no es lo mismo que hacerlo hacia el 1900: los precios de los productos primarios argentinos **cayeron ocho veces** en el siglo, lo que nos bajó **del quinto puesto** en el ranking de países **al lugar número 50**.

La idea que en su época planteaba la llamada generación del 80 acerca de convertir a la Argentina en un **país agroexportador** no era desacertada. Pero el desafío actual es

implementar una revolución tecnológica. Creemos que sí, y ése es el corazón del estudio **Argentina digital**, que recientemente presentamos.

La propuesta no consiste solamente en **promover el comercio electrónico**, introducir **Internet en las escuelas** o incorporar **computadoras en la función pública**. Es eso y mucho más: propone pensar un cambio en el perfil de país haciendo hincapié con un fortísimo apoyo a las nuevas **tecnologías de la información**. Tanto para promover exportaciones de servicios como para competir mejor.

Esta es la propuesta de máxima, si se acepta que puede adaptarse bien a nuestro país y si los costados negativos (que los tienen) pueden controlarse o minimizarse. Basta citar el ejemplo de la India, Israel e Irlanda, que hicieron crecer sus exportaciones de servicios de informática hasta convertirlos en una porción importante de su economía. Algo parecido pasó, más recientemente, en países como Costa Rica y República Dominicana.

Apostamos a que nuestra idiosincrasia nos permita tener **ventajas comparativas** por nuestra forma de ser, nuestro nivel cultural, conocimientos de idiomas y también porque tenemos excelentes dotes de imaginación.

Se trata de una decisión estratégica para el país y, por eso, no es resorte de los técnicos sino **de los políticos**. Y más aún, de los estadistas: tal es la importancia de los temas involucrados, que el desarrollo de este tipo de iniciativas trascendió el ámbito de los laboratorios informáticos para figurar entre los puntos más importantes en las agendas de los presidentes de los países más avanzados.

El estudio **Argentina digital** señala como preocupante que este comienzo de siglo no encuentre al país preparado para afrontar el desafío de la **era de la información**. Esto se debe a dos causas. Por un lado, hay un evidente problema cultural de nuestros dirigentes políticos, académicos y empresariales, que parecen no percibir el cambio de era.

Por otro, falta un plan maestro, **una estrategia global**. En esta materia, iniciativas y esfuerzos aislados sólo conducen a resultados incoordinados y estériles. En cambio, un plan común crea sinergia, **fomenta las inversiones** y orienta a los ciudadanos.

El proyecto **Argentina digital** intenta promover el ingreso del país en la **sociedad de la información**. En forma gradual pero sin pausa, abarcando todos los ámbitos y sectores. Nuestro estudio fue apurado para acercar propuestas al nuevo gobierno. La crítica situación económica actual exige nuevas ideas, especialmente aquellas factibles de realizar, donde las grandes inversiones -en dinero pero especialmente en imaginación- deben provenir del sector privado y de los ciudadanos. En Inglaterra, por ejemplo, la Fundación de Bill Gates reparte PC entre los desempleados.

Pero si bien las inversiones deberán ser realizadas por el sector privado, el Gobierno tiene un importante rol de liderazgo que cumplir. La propuesta que planteamos apunta a **agrandar el mercado**, lo que será una buena noticia para los sectores informáticos. Sería bueno que esta oportunidad no se pierda. Si fuera así, al menos que sea por una decisión meditada, pero nunca por descuido o desidia.

Miércoles 24 de Mayo de 2000

## La transición a la economía digital

Por Horacio M. Lynch y Mauricio Devoto

Para *La Nación*

EN el curso de una investigación, tropezamos con un reciente estudio de Nueva Zelanda denominado *La economía del conocimiento*, con un capítulo inicial cuyo título, por razones obvias, nos llamó la atención: "Venciendo la enfermedad argentina". Según sus autores, la enfermedad argentina consiste en la decadencia de un país próspero que de pronto desapareció de los primeros lugares, y recuerdan que, a pesar de que hoy la Argentina es considerada un país en vías de desarrollo, en 1929 figuraba entre los primeros del mundo, por encima de los más importantes de Europa. Y el capítulo tiene un subtítulo con un "llamado de atención" para que a Nueva Zelanda no le ocurra lo mismo.

Las similitudes entre la situación de nuestros países, salvando las distancias en favor de aquél, justifican glosar el trabajo. Los autores opinan que Nueva Zelanda debe ser cautelosamente optimista al llegar al tercer milenio. Comentan los logros alcanzados desde mediados de los años 80, en que el país se embarcó en un programa de reformas económicas que lo han transformado en una de las economías más abiertas, transparentes y desreguladas del mundo, y, aunque en una posición mucho más avanzada que la Argentina, se formulan ese severo llamado de atención.

Preocupa a los neozelandeses que sus competidores estén jugando a un juego diferente, cuyas reglas les cuesta aprender, y, más aún, que los hombres de negocios y el gobierno no lo adviertan o no quieran reconocerlo. Temen así perder todo lo ganado en los últimos años, a menos que tomen la gran decisión: la conversión de Nueva Zelanda de una economía pastoril a la nueva economía del conocimiento.

Parece innecesario agregar algo a tan simple explicación que se reproduce exactamente para nuestro país.

Dice el estudio que los neozelandeses todavía no han advertido que Internet es el equivalente moderno del buque frigorífico que revolucionó su economía en el siglo XIX. Entrando en el siglo XXI, Internet será el nuevo buque que les permitirá alcanzar los mercados mundiales.

Cincuenta años atrás, Nueva Zelanda exportaba la mayoría de sus productos primarios a Gran Bretaña y el país avanzaba hacia la prosperidad detrás de sus ovejas. Tuvieron el tercer ingreso per cápita del mundo, pero hoy están apenas por encima de Grecia y Portugal, al final de los países de la Comunidad Europea. Se preguntan, entonces, los autores: "¿Cómo hemos caído tanto en el *ranking*? ¿Será que nos hemos contagiado la enfermedad argentina?"

Como se advierte, si cambiamos ovejas por vacas, la similitud es asombrosa, recordando que la Argentina hoy en día está aún más abajo en el *ranking* mundial.

Para los autores del estudio, la respuesta es que Nueva Zelanda está todavía jugando el juego de la exportación de *commodities*. Y comentan todo lo que se ha hecho por mejorar al máximo este esquema. Pero el esquema parece agotado. La comparación es válida con nuestro país, pues hemos mejorado notablemente nuestra eficiencia ampliando las áreas sembradas,

incorporando nuevos cultivos, mejorando las cosechas año tras año, refinando el ganado y hasta logrando la eliminación de la aftosa.

Faltaría agregar que, según Peter Drucker, la explicación reside en que durante el siglo XX los productos que exportan tanto Nueva Zelanda como la Argentina perdieron diez veces su valor.

### **El síndrome de Nueva Zelanda**

Continúa diciendo el informe que Nueva Zelanda, aunque contando con muy buenas bases para triunfar en la economía global, todavía no ha efectuado la transición de una economía agrícola a otra basada en la información, donde el conocimiento es el componente más significativo de los productos.

Insisten en que los neozelandeses todavía no han aprendido, como muchos de sus competidores ya lo han hecho, la necesidad de contar con una "plataforma de exportación del conocimiento":

"Nuestros competidores -Irlanda, Singapur, Australia, Gran Bretaña- lo han hecho y están venciéndonos en el juego de la economía de la prosperidad".

El estudio termina afirmando que, de no prestar atención al tema, continuarán cayendo en el *ranking*, quizá tan bajo como Eslovenia y Hungría, países que hoy envidian el estándar de vida de Nueva Zelanda, y que dentro de diez años los economistas la mencionarán como uno de esos infortunados países que fallaron en la transición de sus economías. Esta situación, ironizan, podría denominarse "el síndrome de Nueva Zelanda". Y exhortan a moverse rápido hacia la nueva economía, a riesgo de ser incluidos entre los perdedores.

También nosotros estamos dejando pasar una nueva oportunidad. Si Nueva Zelanda, en mejor condición, está tan preocupada, ¿qué puede esperarnos a los argentinos?

La cita inicial de Drucker resume nuestro planteo. Nuestro principal obstáculo es la brecha cultural de la dirigencia argentina, que, al igual que sus pares neozelandeses, no comprende las enormes implicancias de lo que está ocurriendo en el mundo.

### **La enfermedad argentina**

El nuevo gobierno ha dado muestras de haber percibido la situación, moviéndose rápido pero no tanto como exige el momento ni con la profundidad necesaria para entender la verdadera esencia de un cambio en que Internet no es más que la cara visible de una verdadera revolución, de un cambio de era que impactará fuertemente en las sociedades y en las economías, y que esto está demandando un nuevo proyecto, un nuevo perfil para nuestro país.

A principios del siglo XX, la Argentina tuvo su proyecto agrícola-ganadero- exportador. Luego de la prosperidad alcanzada, e incluso pese a los esfuerzos realizados, dicho proyecto mostró su agotamiento en las últimas décadas por la pérdida de valor de nuestros productos (nos excusábamos culpando a un "deterioro de los términos de intercambio" que maliciosamente nos imponían los países centrales, en lugar de reconocer que debíamos cambiar).

Todavía tenemos la oportunidad de cambiar. Es, pues, imperioso que la Argentina haga su transición, diseñando un nuevo proyecto que le permita ingresar con posibilidades en el nuevo siglo.

**Horacio M. Lynch y Mauricio Devoto son directores del Centro de Investigaciones en Information Technology, autores del libro *Argentina digital*, Cenit, 1999.**

## **LEYES Y DECRETOS**

### **FIRMA DIGITAL**

#### **Ley 25.506**

Consideraciones generales. Certificados digitales. Certificador licenciado. Titular de un certificado digital. Organización institucional. Autoridad de aplicación. Sistema de auditoría. Comisión Asesora para la Infraestructura de Firma Digital. Responsabilidad. Sanciones. Disposiciones Complementarias

Sancionada: Noviembre 14 de 2001. Promulgada de Hecho: Diciembre 11 de 2001. El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

### **LEY DE FIRMA DIGITAL**

#### **CAPITULO I**

##### **Consideraciones generales**

**ARTICULO 1º** - Objeto. Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley.

**ARTÍCULO 2º** - Firma Digital. Se entiende por firma digital al 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 firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.

**ARTICULO 3º** - Del requerimiento de firma. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia.

**ARTÍCULO 4º** - Exclusiones. Las disposiciones de esta ley no son aplicables:

- a) *A las disposiciones por causa de muerte;*
- b) *A los actos jurídicos del derecho de familia;*
- c) *A los actos personalísimos en general;*

*d) A los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes.*

**ARTÍCULO 5º** - Firma electrónica. Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

**ARTÍCULO 6º** - Documento digital. Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.

**ARTÍCULO 7º** - Presunción de autoría. Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma.

**ARTÍCULO 8º** - Presunción de integridad. Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma.

**ARTÍCULO 9º** - Validez. Una firma digital es válida si cumple con los siguientes requisitos:

*a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante;*

*b) Ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente;*

*c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado.*

**ARTICULO 10.** - Remitente. Presunción. Cuando un documento digital sea enviado en forma automática por un dispositivo programado y lleve la firma digital del remitente se presumirá, salvo prueba en contrario, que el documento firmado proviene del remitente.

**ARTICULO 11.** - Original. Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación.

**ARTICULO 12.** - Conservación. La exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción.

## **CAPITULO II**

### **De los certificados digitales**

**ARTICULO 13.** - Certificado digital. Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.

**ARTICULO 14.** - Requisitos de validez de los certificados digitales. Los certificados digitales para ser válidos deben:

*a) Ser emitidos por un certificador licenciado por el ente licenciante;*

*b) Responder a formatos estándares reconocidos internacionalmente, fijados por la autoridad de aplicación, y contener, como mínimo, los datos que permitan:*

*1. Identificar indubitablemente a su titular y al certificador licenciado que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única;*

*2. Ser susceptible de verificación respecto de su estado de revocación;*

*3. Diferenciar claramente la información verificada de la no verificada incluidas en el certificado;*

*4. Contemplar la información necesaria para la verificación de la firma;*

*5. Identificar la política de certificación bajo la cual fue emitido.*

**ARTICULO 15.** - Período de vigencia del certificado digital. A los efectos de esta ley, el certificado digital es válido únicamente dentro del período de vigencia, que comienza en la fecha de inicio y finaliza en su fecha de vencimiento, debiendo ambas ser indicadas en el certificado digital, o su revocación si fuere revocado.

La fecha de vencimiento del certificado digital referido en el párrafo anterior en ningún caso puede ser posterior a la del vencimiento del certificado digital del certificador licenciado que lo emitió.

La Autoridad de Aplicación podrá establecer mayores exigencias respecto de la determinación exacta del momento de emisión, revocación y vencimiento de los certificados digitales.

**ARTICULO 16.** - Reconocimiento de certificados extranjeros. Los certificados digitales emitidos por certificadores extranjeros podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley y sus normas reglamentarias cuando:

*a) Reúnan las condiciones que establece la presente ley y la reglamentación correspondiente para los certificados emitidos por certificadores nacionales y se encuentre vigente un acuerdo de reciprocidad firmado por la República Argentina y el país de origen del certificador extranjero,*

*b) Tales certificados sean reconocidos por un certificador licenciado en el país, que garantice su validez y vigencia conforme a la presente ley. A fin de tener efectos, este reconocimiento deberá ser validado por la autoridad de aplicación.*

### **CAPITULO III**

#### **Del certificador licenciado**

**ARTICULO 17.** - Del certificador licenciado. Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante.

La actividad de los certificadores licenciados no pertenecientes al sector público se prestará en régimen de competencia. El arancel de los servicios prestados por los certificadores licenciados será establecido libremente por éstos.

**ARTICULO 18.** - Certificados por profesión. Las entidades que controlan la matrícula, en relación a la prestación de servicios profesionales, podrán emitir certificados digitales en lo referido a esta función, con igual validez y alcance jurídico que las firmas efectuadas en forma manuscrita. A ese efecto deberán cumplir los requisitos para ser certificador licenciado.

**ARTICULO 19.** - Funciones. El certificador licenciado tiene las siguientes funciones:

a) Recibir una solicitud de emisión de certificado digital, firmada digitalmente con los correspondientes datos de verificación de firma digital del solicitante;

b) Emitir certificados digitales de acuerdo a lo establecido en sus políticas de certificación, y a las condiciones que la autoridad de aplicación indique en la reglamentación de la presente ley;

c) Identificar inequívocamente los certificados digitales emitidos;

d) Mantener copia de todos los certificados digitales emitidos, consignando su fecha de emisión y de vencimiento si correspondiere, y de sus correspondientes solicitudes de emisión;

e) Revocar los certificados digitales por él emitidos en los siguientes casos, entre otros que serán determinados por la reglamentación:

*1) A solicitud del titular del certificado digital.*

*2) Si determinara que un certificado digital fue emitido en base a una información falsa, que en el momento de la emisión hubiera sido objeto de verificación.*

*3) Si determinara que los procedimientos de emisión y/o verificación han dejado de ser seguros.*

*4) Por condiciones especiales definidas en su política de certificación.*

*5) Por resolución judicial o de la autoridad de aplicación.*

f) Informar públicamente el estado de los certificados digitales por él emitidos. Los certificados digitales revocados deben ser incluidos en una lista de certificados revocados indicando fecha y hora de la revocación. La validez y autoría de dicha lista de certificados revocados deben ser garantizadas.

**ARTICULO 20.** - Licencia. Para obtener una licencia el certificador debe cumplir con los requisitos establecidos por la ley y tramitar la solicitud respectiva ante el ente licenciante, el que otorgará la licencia previo dictamen legal y técnico que acredite la aptitud para cumplir con sus funciones y obligaciones. Estas licencias son intransferibles.

**ARTICULO 21.** - Obligaciones. Son obligaciones del certificador licenciado:

- a) Informar a quien solicita un certificado con carácter previo a su emisión y utilizando un medio de comunicación las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de un sistema de licenciamiento y los procedimientos, forma que garantiza su posible responsabilidad patrimonial y los efectos de la revocación de su propio certificado digital y de la licencia que le otorga el ente licenciante. Esa información deberá estar libremente accesible en lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;
- b) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder bajo ninguna circunstancia, a los datos de creación de firma digital de los titulares de certificados digitales por él emitidos;
- c) Mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación;
- d) Operar utilizando un sistema técnicamente confiable de acuerdo con lo que determine la autoridad de aplicación;
- e) Notificar al solicitante las medidas que está obligado a adoptar para crear firmas digitales seguras y para su verificación confiable, y las obligaciones que asume por el solo hecho de ser titular de un certificado digital;
- f) Recabar únicamente aquellos datos personales del titular del certificado digital que sean necesarios para su emisión, quedando el solicitante en libertad de proveer información adicional;
- g) Mantener la confidencialidad de toda información que no figure en el certificado digital;
- h) Poner a disposición del solicitante de un certificado digital toda la información relativa a su tramitación;
- i) Mantener la documentación respaldatoria de los certificados digitales emitidos, por diez (10) años a partir de su fecha de vencimiento o revocación;
- j) Incorporar en su política de certificación los efectos de la revocación de su propio certificado digital y/o de la licencia que le otorgara la autoridad de aplicación;
- k) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, la lista de certificados digitales revocados, las políticas de certificación, la información relevante de los informes de la última auditoría de que hubiera sido objeto, su manual de procedimientos y toda información que determine la autoridad de aplicación;
- l) Publicar en el Boletín Oficial aquellos datos que la autoridad de aplicación determine;
- m) Registrar las presentaciones que le sean formuladas, así como el trámite conferido a cada una de ellas;

- n) Informar en las políticas de certificación si los certificados digitales por él emitidos requieren la verificación de la identidad del titular;
- o) Verificar, de acuerdo con lo dispuesto en su manual de procedimientos, toda otra información que deba ser objeto de verificación, la que debe figurar en las políticas de certificación y en los certificados digitales;
- p) Solicitar inmediatamente al ente licenciante la revocación de su certificado, o informarle la revocación del mismo, cuando existieren indicios de que los datos de creación de firma digital que utiliza hubiesen sido comprometidos o cuando el uso de los procedimientos de aplicación de los datos de verificación de firma digital en él contenidos hayan dejado de ser seguros;
- q) Informar inmediatamente al ente licenciante sobre cualquier cambio en los datos relativos a su licencia;
- r) Permitir el ingreso de los funcionarios autorizados de la autoridad de aplicación, del ente licenciante o de los auditores a su local operativo, poner a su disposición toda la información necesaria y proveer la asistencia del caso;
- s) Emplear personal idóneo que tenga los conocimientos específicos, la experiencia necesaria para proveer los servicios ofrecidos y en particular, competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma digital y experiencia adecuada en los procedimientos de seguridad pertinentes;
- t) Someter a aprobación del ente licenciante el manual de procedimientos, el plan de seguridad y el de cese de actividades, así como el detalle de los componentes técnicos a utilizar;
- u) Constituir domicilio legal en la República Argentina;
- v) Disponer de recursos humanos y tecnológicos suficientes para operar de acuerdo a las exigencias establecidas en la presente ley y su reglamentación;
- w) Cumplir con toda otra obligación emergente de su calidad de titular de la licencia adjudicada por el ente licenciante.

**ARTICULO 22.** - Cese del certificador. El certificador licenciado cesa en tal calidad:

- a) *Por decisión unilateral comunicada al ente licenciante;*
- b) *Por cancelación de su personería jurídica;*
- c) *Por cancelación de su licencia dispuesta por el ente licenciante.*

La autoridad de aplicación determinará los procedimientos de revocación aplicables en estos casos.

**ARTICULO 23.** - Desconocimiento de la validez de un certificado digital. Un certificado digital no es válido si es utilizado:

- a) Para alguna finalidad diferente a los fines para los cuales fue extendido;

- b) Para operaciones que superen el valor máximo autorizado cuando corresponda;
- c) Una vez revocado.

## **CAPITULO IV**

### **Del titular de un certificado digital**

**ARTICULO 24.** - Derechos del titular de un certificado digital. El titular de un certificado digital tiene los siguientes derechos:

- a) A ser informado por el certificador licenciado, con carácter previo a la emisión del certificado digital, y utilizando un medio de comunicación sobre las condiciones precisas de utilización del certificado digital, sus características y efectos, la existencia de este sistema de licenciamiento y los procedimientos asociados. Esa información deberá darse por escrito en un lenguaje fácilmente comprensible. La parte pertinente de dicha información estará también disponible para terceros;*
- b) A que el certificador licenciado emplee los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por él, y a ser informado sobre ello;*
- c) A ser informado, previamente a la emisión del certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago;*
- d) A que el certificador licenciado le informe sobre su domicilio en la República Argentina, y sobre los medios a los que puede acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema, o presentar sus reclamos;*
- e) A que el certificador licenciado proporcione los servicios pactados, y a no recibir publicidad comercial de ningún tipo por intermedio del certificador licenciado.*

**ARTICULO 25.** - Obligaciones del titular del certificado digital. Son obligaciones del titular de un certificado digital:

- a) Mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos, e impedir su divulgación;*
- b) Utilizar un dispositivo de creación de firma digital técnicamente confiable;*
- c) Solicitar la revocación de su certificado al certificador licenciado ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma;*
- d) Informar sin demora al certificador licenciado el cambio de alguno de los datos contenidos en el certificado digital que hubiera sido objeto de verificación.*

## **CAPITULO V**

### **De la organización institucional**

**ARTICULO 26.** - Infraestructura de Firma Digital. Los certificados digitales regulados por esta ley deben ser emitidos o reconocidos, según lo establecido por el artículo 16, por un certificador licenciado.

**ARTICULO 27.** - Sistema de Auditoría. La autoridad de aplicación, con el concurso de la Comisión Asesora para la Infraestructura de Firma Digital, diseñará un sistema de auditoría para evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y disponibilidad de los datos, así como también el cumplimiento de las especificaciones del manual de procedimientos y los planes de seguridad y de contingencia aprobados por el ente licenciante.

**ARTICULO 28.** - Comisión Asesora para la Infraestructura de Firma Digital. Créase en el ámbito jurisdiccional de la Autoridad de Aplicación, la Comisión Asesora para la Infraestructura de Firma Digital.

## **CAPITULO VI**

### **De la autoridad de aplicación**

**ARTICULO 29.** - Autoridad de Aplicación. La autoridad de aplicación de la presente ley será la Jefatura de Gabinete de Ministros.

**ARTICULO 30.** - Funciones. La autoridad de aplicación tiene las siguientes funciones:

- a) Dictar las normas reglamentarias y de aplicación de la presente;*
- b) Establecer, previa recomendación de la Comisión Asesora para la Infraestructura de la Firma Digital, los estándares tecnológicos y operativos de la Infraestructura de Firma Digital;*
- c) Determinar los efectos de la revocación de los certificados de los certificadores licenciados o del ente licenciante;*
- d) Instrumentar acuerdos nacionales e internacionales a fin de otorgar validez jurídica a las firmas digitales creadas sobre la base de certificados emitidos por certificadores de otros países;*
- e) Determinar las pautas de auditoría, incluyendo los dictámenes tipo que deban emitirse como conclusión de las revisiones;*
- f) Actualizar los valores monetarios previstos en el régimen de sanciones de la presente ley;*
- g) Determinar los niveles de licenciamiento;*
- h) Otorgar o revocar las licencias a los certificadores licenciados y supervisar su actividad, según las exigencias instituidas por la reglamentación;*
- i) Fiscalizar el cumplimiento de las normas legales y reglamentarias en lo referente a la actividad de los certificadores licenciados;*
- j) Homologar los dispositivos de creación y verificación de firmas digitales, con ajuste a las normas y procedimientos establecidos por la reglamentación;*
- k) Aplicar las sanciones previstas en la presente ley.*

**ARTICULO 31.** - Obligaciones. En su calidad de titular de certificado digital, la autoridad de aplicación tiene las mismas obligaciones que los titulares de certificados y que los certificadores licenciados. En especial y en particular debe:

*a) Abstenerse de generar, exigir, o por cualquier otro medio tomar conocimiento o acceder, bajo ninguna circunstancia, a los datos utilizados para generar la firma digital de los certificadores licenciados;*

*b) Mantener el control exclusivo de los datos utilizados para generar su propia firma digital e impedir su divulgación;*

*c) Revocar su propio certificado frente al compromiso de la privacidad de los datos de creación de firma digital;*

*d) Publicar en Internet o en la red de acceso público de transmisión o difusión de datos que la sustituya en el futuro, en forma permanente e ininterrumpida, los domicilios, números telefónicos y direcciones de Internet tanto de los certificadores licenciados como los propios y su certificado digital;*

*e) Supervisar la ejecución del plan de cese de actividades de los certificadores licenciados que discontinúan sus funciones.*

**ARTICULO 32.** - Arancelamiento. La autoridad de aplicación podrá cobrar un arancel de licenciamiento para cubrir su costo operativo y el de las auditorias realizadas por sí o por terceros contratados a tal efecto.

## **CAPITULO VII**

### **Del sistema de auditoria**

**ARTICULO 33.** - Sujetos a auditar. El ente licenciante y los certificadores licenciados, deben ser auditados periódicamente, de acuerdo al sistema de auditoria que diseñe y apruebe la autoridad de aplicación.

La autoridad de aplicación podrá implementar el sistema de auditoria por sí o por terceros habilitados a tal efecto. Las auditorias deben como mínimo evaluar la confiabilidad y calidad de los sistemas utilizados, la integridad, confidencialidad y, disponibilidad de los datos, así como también el cumplimiento de las especificaciones del manual de procedimientos y los planes de seguridad y, de contingencia aprobados por el ente licenciante.

**ARTICULO 34.** - Requisitos de habilitación. Podrán ser terceros habilitados para efectuar las auditorias las Universidades y organismos científicos y/o tecnológicos nacionales o provinciales, los Colegios y Consejos profesionales que acrediten experiencia profesional acorde en la materia.

## **CAPITULO VIII**

### **De la Comisión Asesora para la Infraestructura de Firma Digital**

**ARTICULO 35.** - Integración y funcionamiento. La Comisión Asesora para la Infraestructura de Firma Digital estará integrada multidisciplinariamente por un máximo de 7 (siete) profesionales de carreras afines a la actividad de reconocida trayectoria y experiencia,

provenientes de Organismos del Estado nacional, Universidades Nacionales y Provinciales, Cámaras, Colegios u otros entes representativos de profesionales.

Los integrantes serán designados por el Poder Ejecutivo por un período de cinco (5) años renovables por única vez.

Se reunirá como mínimo trimestralmente. Deberá expedirse prontamente a solicitud de la autoridad de aplicación y sus recomendaciones y disidencias se incluirán en las actas de la Comisión.

Consultará periódicamente mediante audiencias públicas con las cámaras empresarias, los usuarios y las asociaciones de consumidores y mantendrá a la autoridad de aplicación regularmente informada de los resultados de dichas consultas.

**ARTICULO 36.** - Funciones. La Comisión debe emitir recomendaciones por iniciativa propia o a solicitud de la autoridad de aplicación, sobre los siguientes aspectos:

- a) *Estándares tecnológicos;*
- b) *Sistema de registro de toda la información relativa a la emisión de certificados digitales;*
- c) *Requisitos mínimos de información que se debe suministrar a los potenciales titulares de certificados digitales de los términos de las políticas de certificación;*
- d) *Metodología y requerimiento del resguardo físico de la información;*
- e) *Otros que le sean requeridos por la autoridad de aplicación.*

## **CAPITULO IX**

### **Responsabilidad**

**ARTICULO 37.** - Convenio de partes. La relación entre el certificador licenciado que emita un certificado digital y el titular de ese certificado se rige por el contrato que celebren entre ellos, sin perjuicio de las previsiones de la presente ley, y demás legislación vigente.

**ARTICULO 38.** - Responsabilidad de los certificadores licenciados ante terceros. El certificador que emita un certificado digital o lo reconozca en los términos del artículo 16 de la presente ley, es responsable por los daños y perjuicios que provoque, por los incumplimientos a las previsiones de ésta, por los errores u omisiones que presenten los certificados digitales que expida, por no revocarlos, en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos de certificación exigibles. Corresponderá al prestador del servicio demostrar que actuó con la debida diligencia.

**ARTICULO 39.** - Limitaciones de responsabilidad. Los certificadores licenciados no son responsables en los siguientes casos:

- a) *Por los casos que se excluyan taxativamente en las condiciones de emisión y utilización de sus certificados y que no estén expresamente previstos en la ley;*

*b) Por los daños y perjuicios que resulten del uso no autorizado de un certificado digital, si en las correspondientes condiciones de emisión y utilización de sus certificados constan las restricciones de su utilización;*

*c) Por eventuales inexactitudes en el certificado que resulten de la información facilitada por el titular que, según lo dispuesto en las normas y en los manuales de procedimientos respectivos, deba ser objeto de verificación, siempre que el certificador pueda demostrar que ha tomado todas las medidas razonables.*

## **CAPITULO X**

### **Sanciones**

**ARTICULO 40.** - Procedimiento. La instrucción sumarial y la aplicación de sanciones por violación a disposiciones de la presente ley serán realizadas por el ente licenciante. Es aplicable la Ley de Procedimientos Administrativos 19.549 y sus normas reglamentarias.

**ARTICULO 41.** - Sanciones. El incumplimiento de las obligaciones establecidas en la presente ley para los certificadores licenciados dará lugar a la aplicación de las siguientes sanciones:

*a) Apercibimiento;*

*b) Multa de pesos diez mil (\$ 10.000) a pesos quinientos mil (\$ 500.000);*

*c) Caducidad de la licencia.*

Su gradación según reincidencia y/u oportunidad serán establecidas por la reglamentación. El pago de la sanción que aplique el ente licenciante no relevará al certificador licenciado de eventuales reclamos por daños y perjuicios causados a terceros y/o bienes de propiedad de éstos, como consecuencia de la ejecución del contrato que celebren y/o por el incumplimiento de las obligaciones asumidas conforme al mismo y/o la prestación del servicio.

**ARTICULO 42.** - Apercibimiento. Podrá aplicarse sanción de apercibimiento en los siguientes casos:

*a) Emisión de certificados sin contar con la totalidad de los datos requeridos, cuando su omisión no invalidare el certificado;*

*b) No facilitar los datos requeridos por el ente licenciante en ejercicio de sus funciones;*

*c) Cualquier otra infracción a la presente ley que no tenga una sanción mayor.*

**ARTICULO 43.** - Multa. Podrá aplicarse sanción de multa en los siguientes casos:

*a) Incumplimiento de las obligaciones previstas en el artículo 21;*

*b) Si la emisión de certificados se realizare sin cumplimentar las políticas de certificación comprometida y causare perjuicios a los usuarios, signatarios o terceros, o se afectare gravemente la seguridad de los servicios de certificación;*

*c) Omisión de llevar el registro de los certificados expedidos;*

*d) Omisión de revocar en forma o tiempo oportuno un certificado cuando así correspondiere;*

*e) Cualquier impedimento u obstrucción a la realización de inspecciones o auditorias por parte de la autoridad de aplicación y del ente licenciante;*

*f) Incumplimiento de las normas dictadas por la autoridad de aplicación;*

*g) Reincidencia en la comisión de infracciones que dieran lugar a la sanción de apercibimiento.*

**ARTICULO 44.** - Caducidad. Podrá aplicarse la sanción de caducidad de la licencia en caso de:

*a) No tomar los debidos recaudos de seguridad en los servicios de certificación;*

*b) Expedición de certificados falsos;*

*c) Transferencia no autorizada o fraude en la titularidad de la licencia;*

*d) Reincidencia en la comisión de infracciones que dieran lugar a la sanción de multa;*

*e) Quiebra del titular.*

La sanción de caducidad inhabilita a la titular sancionada y a los integrantes de órganos directivos por el término de 10 años para ser titular de licencias.

**ARTICULO 45.** - Recurribilidad. Las sanciones aplicadas podrán ser recurridas ante los Tribunales Federales con competencia en lo Contencioso Administrativo correspondientes al domicilio de la entidad, una vez agotada la vía administrativa pertinente.

La interposición de los recursos previstos en este capítulo tendrá efecto devolutivo.

**ARTICULO 46.** - Jurisdicción. En los conflictos entre particulares y certificadores licenciados es competente la Justicia en lo Civil y Comercial Federal. En los conflictos en que sea parte un organismo público certificador licenciado, es competente la Justicia en lo Contencioso-administrativo Federal.

## **CAPITULO XI**

### **Disposiciones Complementarias**

**ARTICULO 47.** - Utilización por el Estado Nacional. El Estado nacional utilizará las tecnologías y previsiones de la presente ley en su ámbito interno y en relación con los administrados de acuerdo con las condiciones que se fijen reglamentariamente en cada uno de sus poderes.

**ARTICULO 48.** - Implementación. El Estado nacional, dentro de las jurisdicciones y entidades comprendidas en el artículo 8º de la Ley 24.156, promoverá el uso masivo de la firma digital de tal forma que posibilite el trámite de los expedientes por vías simultáneas, búsquedas automáticas de la información y seguimiento y control por parte del interesado, propendiendo a la progresiva despapelización.

En un plazo máximo de 5 (cinco) años contados a partir de la entrada en vigencia de la presente ley, se aplicará la tecnología de firma digital a la totalidad de las leyes, decretos,

decisiones administrativas, resoluciones y sentencias emanados de las jurisdicciones y entidades comprendidas en el artículo 8° de la Ley 24.156.

**ARTICULO 49.** - Reglamentación. El Poder Ejecutivo deberá reglamentar esta ley en un plazo no mayor a los 180 (ciento ochenta) días de su publicación en el Boletín Oficial de la Nación.

**ARTICULO 50.** - Invitación. Invítase a las jurisdicciones provinciales a dictar los instrumentos legales pertinentes para adherir a la presente ley.

**ARTICULO 51.** - Equiparación a los efectos del derecho penal. Incorporase el siguiente texto como artículo 78 (bis) del Código Penal:

Los términos firma y suscripción comprenden la firma digital, la creación de una firma digital o firmar digitalmente. Los términos documento, instrumento privado y certificado comprenden el documento digital firmado digitalmente.

**ARTICULO 52.** - Autorización al Poder Ejecutivo. Autorízase al Poder Ejecutivo para que por la vía del artículo 99, inciso 2, de la Constitución Nacional actualice los contenidos del Anexo de la presente ley a fin de evitar su obsolescencia.

**A**

**ARTICULO 53.** - Comuníquese al Poder Ejecutivo.

DADA EN LA SALA DE SESIONES DEL CONGRESO ARGENTINO, EN BUENOS AIRES, A LOS CATORCE DIAS DEL MES DE NOVIEMBRE DEL AÑO DOS MIL UNO.

- REGISTRADA BAJO EL N° 25.506 -

Rafael Pascual. - Eduardo Menem. - Guillermo Aramburu. - Juan C. Oyarzún.

## ANEXO

Información: conocimiento adquirido acerca de algo o alguien.

Procedimiento de verificación: proceso utilizado para determinar la validez de una firma digital. Dicho proceso debe considerar al menos:

*a) que dicha firma digital ha sido creada durante el período de validez del certificado digital del firmante;*

*b) que dicha firma digital ha sido creada utilizando los datos de creación de firma digital correspondientes a los datos de verificación de firma digital indicados en el certificado del firmante;*

*c) la verificación de la autenticidad y la validez de los certificados involucrados.*

Datos de creación de firma digital: datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear su firma digital.

Datos de verificación de firma digital: datos únicos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma digital, la integridad del documento digital y la identidad del firmante.

Dispositivo de creación de firma digital: dispositivo de hardware o software técnicamente confiable que permite firmar digitalmente.

Dispositivo de verificación de firma digital: dispositivo de hardware o software técnicamente confiable que permite verificar la integridad del documento digital y la identidad del firmante.  
Políticas de certificación: reglas en las que se establecen los criterios de emisión y utilización de los certificados digitales.

Técnicamente confiable: cualidad del conjunto de equipos de computación, software, protocolos de comunicación y de seguridad y procedimientos administrativos relacionados que cumplan los siguientes requisitos:

- 1. Resguardar contra la posibilidad de intrusión y/o uso no autorizado;*
- 2. Asegurar la disponibilidad, confiabilidad, confidencialidad y correcto funcionamiento;*
- 3. Ser apto para el desempeño de sus funciones específicas;*
- 4. Cumplir las normas de seguridad apropiadas, acordes a estándares internacionales en la materia;*
- 5. Cumplir con los estándares técnicos y de auditoria que establezca la Autoridad de Aplicación.*

## **FIRMA DIGITAL, DECRETO 724/2006**

### **Decreto 724/2006**

Modifícase la reglamentación de la Ley N° 25.506

Bs. As., 8/6/2006

VISTO la Ley N° 25.506 y el Decreto N° 2628 del 19 de diciembre de 2002, modificado por el Decreto N° 1028 del 6 de noviembre de 2003, y

### **CONSIDERANDO:**

Que la Ley N° 25.506 de Firma Digital reconoce la eficacia jurídica del empleo del documento electrónico, la firma electrónica y la firma digital.

Que el Decreto N° 2628/02 reglamentario de la Ley antes mencionada, establece las condiciones que deben cumplir a tal fin los certificadores que soliciten una licencia.

Que entre dichas condiciones se encuentra la de contar con seguros vigentes acordes con las responsabilidades asumidas, que cumplan con los requisitos establecidos en el mencionado decreto.

Que a fin de eliminar condiciones que resulten gravosas sobre la actividad de certificación, considerando especialmente que se trata de un área de reciente desarrollo, resulta conveniente derogar el artículo 30 del mencionado Decreto.

Que asimismo, el mencionado Decreto contiene disposiciones de aplicación específica a la Administración Pública Nacional, entre las cuales se encuentra la de aceptar en sus aplicaciones certificados digitales de certificadores públicos y privados.

Que en virtud de las capacidades desarrolladas por la propia Administración Pública Nacional en materia de firma digital y con el fin de evitar que se encarezcan innecesariamente las tramitaciones que efectúe la comunidad ante al Estado, resulta conveniente la utilización de certificados emitidos por certificadores licenciados públicos en forma gratuita.

Que conforme surge de la facultad contenida en el artículo 52 de la ley 25.506 se procede a actualizar los contenidos del anexo I correspondiente a dicha normativa definiendo el alcance del término "Tercero Usuario".

Que el artículo 23 de la Ley N° 25.506 de Firma Digital establece el desconocimiento de la validez de un certificado digital si es utilizado para alguna finalidad diferente para la cual fue expedido.

Que en virtud de ello, el tercero usuario tiene derecho a aceptar o rechazar documentos electrónicos firmados digitalmente utilizando certificados cuya política de certificación no reúna las condiciones por él requeridas.

Que a fin de adecuar el decreto reglamentario al espíritu de la Ley 25.506, se considera conveniente modificar su artículo 1° inciso b), reconociendo que los certificados digitales emitidos por certificadores no licenciados permiten verificar firmas electrónicas.

Que ha tomado intervención el servicio jurídico permanente de la jurisdicción.

Que la presente medida se dicta en virtud de lo dispuesto por el artículo 99, inciso 2, de la Constitución de la Nación Argentina.

Por ello,

## **EL PRESIDENTE DE LA NACION ARGENTINA**

### **DECRETA:**

Artículo 1° — Derógase el artículo 30 del Decreto N° 2628 del 19 de diciembre de 2002.

Art. 2° — Sustitúyese el texto del artículo 38 del Decreto N° 2628 del 19 de diciembre de 2002 por el siguiente: "Artículo 38.- Las entidades y jurisdicciones pertenecientes a la Administración Pública Nacional podrán ser certificadores licenciados emitir certificados para agentes y funcionarios públicos y particulares, tanto sean personas físicas como jurídicas. Dichos certificados deberán ser provistos en forma gratuita.

En aquellas aplicaciones en las que la Administración Pública Nacional interactúe con la comunidad, solamente se admitirá la recepción de documentos digitales firmados digitalmente utilizando certificados emitidos por certificadores licenciados o certificados extranjeros reconocidos en los términos del artículo 16 de Ley 25.506."

Art. 3° — Incorporase al Anexo I del Decreto N° 2628 del 19 de diciembre de 2002, la siguiente definición: "18. TERCERO USUARIO: persona física o jurídica que recibe un documento firmado digitalmente y que genera una consulta para verificar la validez del certificado digital correspondiente."

Art. 4° — Incorpórase como artículo 34 bis del Decreto N° 2628 del 19 de diciembre de 2002, el siguiente texto: "Aceptación por parte de terceros usuarios de documentos electrónicos firmados digitalmente. Los terceros usuarios que sean personas jurídicas que implementen aplicaciones que requieran firma digital, tienen la facultad de definir las características y requerimientos que deben cumplir las Políticas de Certificación, a los efectos de aceptar documentos electrónicos firmados digitalmente utilizando certificados digitales amparados por dichas Políticas. Dichas características y requerimientos deben ser manifestados previamente en forma clara y transparente a los titulares de certificados que pretendan operar con ellos."

Art. 5° — Modifícase el texto del artículo 1° inciso b) del Decreto N° 2628 del 19 de diciembre de 2002 por el siguiente: "Artículo 1° inciso b): Firma electrónica basada en certificados digitales emitidos por certificadores no licenciados en el marco de la presente reglamentación".

Art. 6° — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — KIRCHNER. — Alberto A. Fernández. — Alberto J. B. Iribarne.