

PARDO, A.
Documento Electrónico



2005

61150



UNIVERSIDAD NACIONAL DE RÍO CUARTO

FACULTAD DE CIENCIAS ECONÓMICAS

DOCUMENTO ELECTRÓNICO Y FIRMA DIGITAL

ALDO PARDO
DNI: 27570979
DIRECCIÓN: SAN JUAN 544
TELÉFONO: 4622020
E-MAIL: aldopardo1@hotmail.com

CARRERA DE GRADO: CONTADOR PÚBLICO

DIRECTOR: CDOR. EDGARDO PEREYRA

PRESENTACIÓN: 2005

05118



05118

61150

MFN:
Clasif:
E-973

INTRODUCCIÓN

Con el nacimiento de la electrónica y la posibilidad de crear y procesar información a través de pulsos eléctricos se han venido suscitando cambios a una muy alta velocidad, los cuales han generado la posibilidad de controlar otros tiempos y espacios diferentes de los reales.

Las tecnologías de la información constituyen el núcleo central de una transformación multidimensional que experimenta la economía y la sociedad, de aquí lo importante que es el estudio y dominio de las influencias que tal transformación impone al ser humano como ente social, ya que tiende a modificar no sólo sus hábitos y patrones de conducta, sino, incluso, su forma de pensar y de realizar las cosas.

Es tan importante el aporte que hace la nueva tecnología que hasta ha llegado a ser la figura representativa de nuestra cultura, caracterizándola como “la sociedad de la información”.

Lo digital ha permitido la comunicación y distribución de conocimiento a distancia de una manera prácticamente instantánea, aceleración del tiempo histórico, desterritorialización y globalización, surgiendo un nuevo espacio, el cibernético.

El desarrollo acelerado de programas y aplicaciones que se generalizan acercándose más al “gran público”, agradables con el uso de las técnicas de multimedia, hacen que cada vez más personas tengan la posibilidad de utilizarlos.

Estos factores hacen que cada día los costos se reduzcan y por tanto se amplíe el uso de estos medios en otros sectores, no sólo en la academia militar o industrial, sino en el sector empresarial, en la salud, la educación, el ocio y los propios hogares.

Este nuevo espacio y las posibilidades que él brinda, como por ejemplo la factibilidad de poder realizar la representación de hechos y actos que ocurren en la realidad en forma digital, a través de documentos electrónicos, han generado nuevos inconvenientes, como la necesidad de garantizar la autoría, valor probatorio de los mismos, de asegurar que el documento llegó al destinatario exactamente como se lo envió el emisor y su conservación.

Inconvenientes que trajeron consigo el replanteo de ciertos conceptos institucionalizados en la sociedad como la presentación de los documentos en soporte

papel y la utilización de la firma holográfica como único medio para garantizar la autoría del mismo.

La generalización de Internet en la década del '90 acentuó el uso de la transmisión electrónica de datos y con ello, la utilización de los documentos electrónicos para realizar operaciones que hasta entonces se realizaban en forma manual y personal.

Como consecuencia de ello se tuvo que establecer un marco normativo que regulara la utilización de este fenómeno, caracterizado por su utilización a escala mundial. Por lo que, si bien cada país lo regula en forma individual, se utilizan normas similares de manera de brindar homogeneización y posibilidades de crecimiento global. Es así como la mayoría de las normas se basan en la ley de Firma Digital del Estado de Utah de los Estados Unidos y la ley modelo de Uncitral.

Los distintos países fueron adaptando sus legislaciones a medida que se iban informatizando, es por ello que las legislaciones más nuevas son la de los países menos desarrollados.

Es así como en la Argentina surgieron distintas resoluciones que le daban un marco legal a la utilización del documento electrónico y la firma digital, hasta que en el año 2001 se aprobó la Ley 25506 de Firma Digital y Documentos Electrónicos.

La utilización de esta herramienta es de uso cada vez más generalizado. Así como se ha llegado al punto de que la computadora es un instrumento casi indispensable en el trabajo actual, y con la proliferación de Internet, el uso del mismo intercambiando información, por ejemplo, por medio de mail, hace necesario e indispensable el conocimiento de este instrumental, conocer como utilizar documentos electrónicos y la firma digital es necesario y primordial en los tiempos que corren.

Las posibilidades de uso que brinda la firma digital y los documentos electrónicos son innumerables dado que por medio de ellos se puede presentar e intercambiar información con la Administración Pública, desburocratizar y despapelizar las organizaciones, como también realizar contratos donde se realicen declaraciones de voluntad de sujetos que no están presentes físicamente, lo que lleva a la obligación de tener conocimiento del marco legal que lo regula.

El trabajo pretende brindar el conocimiento necesario para la utilización de esta herramienta, cada vez más generalizada y de uso casi indispensable en los negocios, su marco regulatorio y eficacia jurídica de manera que cuando se presente la



posibilidad y con cada vez más frecuencia, como el uso del mail, se tengan los instrumentos necesarios para su aprovechamiento.

La ley 25506 nos brinda el marco normativo y técnico sobre el cual se asienta este complejo sistema de transmisión y conservación de documentos electrónicos, por lo que el estudio de la misma, conjuntamente con distintas aplicaciones específicas del Sector Público nos da una base necesaria para su utilización en forma privada, como también en la presentación e intercambio de información con la Administración Pública.

CAPÍTULO I

Cambio social

El surgimiento de la era digital trajo la necesidad de repensar importantes aspectos relativos a la organización social, la tecnología, la privacidad, la libertad, observándose que muchos de los enfoques se ven seducidos por la novedad, sin darle al tema el análisis que se merece¹.

Las sociedades humanas se caracterizan por el constante cambio, causando una profunda incidencia en el desarrollo de patrones de conducta social, creando entre las personas nuevos modos de interacción. No se trata solo de progreso científico o tecnológico, sino que el cambio involucra las creencias, las actitudes psicológicas, el ámbito económico y político; en suma, la forma de convivir en el mundo. Es decir, estamos viviendo un verdadero cambio social que modifica irreversiblemente los modos de conducta en sociedad.

Los mismos se generan en el afán conciente de las personas por buscar soluciones satisfactorias a sus problemas y necesidades. Es así como nadie podría desconocer que el desarrollo de la ciencia y la tecnología es una de sus importantes causas directas e inmediatas.

La revolución tecnológica ha transformado las relaciones entre los hombres.

Estamos en una sociedad donde las tecnologías de la información han llegado a ser la figura representativa de nuestra cultura, hasta el punto de que para designar el marco de nuestra convivencia se alude reiteradamente a la expresión "sociedad de la información".

Y detrás de todo este desarrollo tecnológico descansa la información como objeto de dicha revolución. La información ya era valiosa en el pasado, significaba encontrarse en una situación ventajosa respecto a quienes no la tenían. Pero en el presente su valor se acrecienta, ya que antes no existía la posibilidad de convertir informaciones parciales y dispersas en informaciones en masa y organizadas, de interrelacionar esa información y de procesarla con rapidez, como ocurre hoy, en la sociedad de la información. En definitiva, lo que ocurre es que esa información cada vez

¹ Lorenzetti, Ricardo. Comercio Electrónico. Ed. Abeledo Perrot. Buenos Aires. Argentina.



aporta más conocimiento, que es lo verdaderamente importante, y que quien dispone de conocimiento tiene poder.

Ello obliga a tener una actitud reflexiva, crítica y responsable ante los nuevos problemas que acarrea la tecnología. Todo nuevo fenómeno tiene aspectos buenos y malos que necesariamente deben ser considerados en su totalidad.

Cambio tecnológico

Los reales avances tecnológicos en la transmisión de datos no comenzaron sino hasta mediados del siglo 19 con la invención del telégrafo, el teléfono y la radio unido a ello la creación por el profesor de Matemática de la Universidad de Cambridge (1833) Charles Babbage de un aparato mecánico capaz de efectuar una cadena de cálculos, esencia del software.

El fin de siglo, en particular ha estado marcado por una convergencia tecnológica hasta el momento independiente. Esta convergencia que experimenta la Electrónica, la Informática y las Telecomunicaciones, tiene su mayor exponente en el vertiginoso crecimiento alcanzado por INTERNET². Como resultado de tal confluencia comienzan a generalizarse nuevos conceptos como: “Tecnología de Información”, “Sociedad del Conocimiento”, “Era de la Información” o “Telemática”.

Las Tecnologías de la Información han sido conceptualizadas como la integración y convergencia de la computación microelectrónica, las telecomunicaciones y la técnica para el procesamiento de datos, sus principales componentes son: el factor humano, los contenidos de la información, el equipamiento, la infraestructura material, el software y los mecanismos de intercambio electrónico de información, los elementos de política y regulaciones y los recursos financieros³.

Las tecnologías de la información constituyen el núcleo central de una transformación que experimenta la economía y la sociedad, de aquí lo importante que es el estudio de las influencias que tal transformación impone al ser humano como ente social, ya que tiende a modificar no sólo sus hábitos y patrones de conducta, sino, incluso, su forma de pensar.

² Caridad Salazar Alca. La informática y su impacto social. Cuba. Obtenido de la página web www.monografias.com

³ González – Manet. Nuevas formas de Comunicación y Cultura: El impacto de las nuevas tecnologías. Editorial Pablo de la Torriente Brau. 1998.



Los factores claves de la transformación han sido⁴:

- Las armas de la microelectrónica que han posibilitado el descomunal avance en la potencia y capacidad de cómputo de los ordenadores.
- Los avances en las telecomunicaciones han provocado explosión del uso de las redes de alcances locales y globales.
- El desarrollo acelerado de programas y aplicaciones que se generalizan acercándose más al “gran publico” mediante interfaces de fácil comunicación, agradables con el uso de las técnicas de multimedia.

Estos factores hacen que cada día los costos se reduzcan y por tanto se amplíe el uso de estos medios en otros sectores, no sólo en la academia militar o industrial, sino en el sector empresarial, en la salud, la educación, el ocio y los propios hogares.

Se considera que en este sector se concentran las mayores inversiones a escala mundial y hasta existen teorías que la consideran como el elemento milagroso, catalizador⁵ a la solución de los problemas económicos sociales.

Esta tecnología no solo actúa hoy como un importante motor del crecimiento porque a sus ventajas económicas en términos de valor añadido, productividad y empleo, se suman otras relacionadas con la posibilidad de permitir la transmisión y generalización de ventajas y experiencias entre diferentes regiones y ambientes. No solo ignora las barreras del tiempo y el espacio ya que sus servicios están las 24 horas y en cualquier rincón del planeta, sino que también modifican las relaciones inter ciudadanos y ésta con las diferentes instituciones.

El acceso a grandes bases de conocimientos en Universidades y Bibliotecas, la enseñanza a distancia, la colaboración desinteresada entre centros de investigación o el empleo de la Telemedicina⁶ son ejemplos del infinito universo de posibilidades que pueden brindar estas tecnologías y que hoy enaltecen la condición humana.

⁴ Caridad Salazar Alea. La informática y su impacto social. Citado en referencia 2

⁵ “capaz de activar y transformar una corriente de opinión o de ideología, o un determinado fenómeno o tendencia humana”. Enciclopedia Salvat. Tomo 3. Ed. Salvat Editores S.A. Barcelona 1978

⁶ “Medicina practicada a distancia por medios informáticos”. Nuevo diccionario enciclopédico ilustrado, Mentor. Ed Sopena Argentina S.A

Redes informáticas

Una red es un conjunto de líneas de cobre, fibras ópticas o señales de microondas que inciden en nodos⁷ y esos nodos a su vez a través de otras líneas se comunican hacia otros nodos, de modo que el nodo más simple es mi propia computadora personal y entonces, todas las computadoras, sin importar el tamaño, se pueden comunicar entre si para intercambiar información de todo tipo.

Con esa idea y como consecuencia de la Guerra Fría (1960-1985), en 1969 surge ARPAnet, que es una Agencia de Proyectos de Investigación Avanzada de Defensa, del Departamento de Defensa de EEUU.

De la misma nace una red experimental en la cual se probaron las teorías y software en los que está basado Internet, la cual no existe en la actualidad.

Esta red gestionada por DARPA, es el origen de Internet, basado en el intento de conectar esta red (ARPAnet) a otras redes mediante enlaces de satélite, radio y cableado.

Es una red experimental que apoya a la investigación militar, en concreto sobre la resistencia a fallos parciales.

La filosofía de esta red consiste en que cada uno de los ordenadores que componen la misma sea capaz de comunicarse, como elemento individual, con cualquier otra computadora de la red.

ARPAnet en principio interconectaba 4 grandes ordenadores en localizaciones secretas de EEUU.

DARPA fue quien diseñó específicamente el protocolo de comunicaciones TCP/IP (Transmission Control Protocol/Internet Protocol), extendido actualmente de forma espectacular.

En 1983 se desarrolla el servidor de nombres (DNS), evitando direcciones numéricas a nivel usuario. Frente al incremento de tráfico, se divide la red en MIL, militar y restringida, y ARPA para el resto de comunicación. La unión de ambas se denomina DARPA.

⁷ Nodos: Vértices o puntos de una red conectados o relacionados de algún modo. Investigación de las operaciones de la empresa. Capítulo IV. Facultad de Ciencias Económicas. Universidad Nacional de Río Cuarto.

Paralelamente, se desarrollan las redes de área local Ethernet con protocolos de comunicación de ARPANet, permitiendo el entendimiento entre redes, apareciendo en 1983 las primeras estaciones de trabajo para escritorio. Estas redes pertenecen a Universidades, Centros de Investigación y Firms Comerciales.

En 1984 la NSF (Fundación Nacional de la Ciencia) intenta hacer uso de ARPANet para facilitar el acceso a cinco Centros de Proceso de Datos, localizados en las principales universidades americanas. Por razones burocráticas no se pudo utilizar ARPANet. El mismo año decide crear su propia red, denominada NSFNet, basada en la tecnología ARPANet, que acabaría convirtiéndose en la auténtica espina dorsal de Internet.

El éxito alcanzado fue tal, que hizo necesaria sucesivas ampliaciones de la capacidad de las líneas troncales. NSFNet, es todavía una de las piezas más importantes dentro de Internet.

Debido al costo de las líneas telefónicas, se decidió crear redes regionales. El tráfico en la red se incrementó con el tiempo hasta la saturación de los ordenadores centrales y líneas telefónicas.

En 1985 se presenta el "Protocolo de Transferencia de Ficheros" (FTP), que sigue vigente en la actualidad.

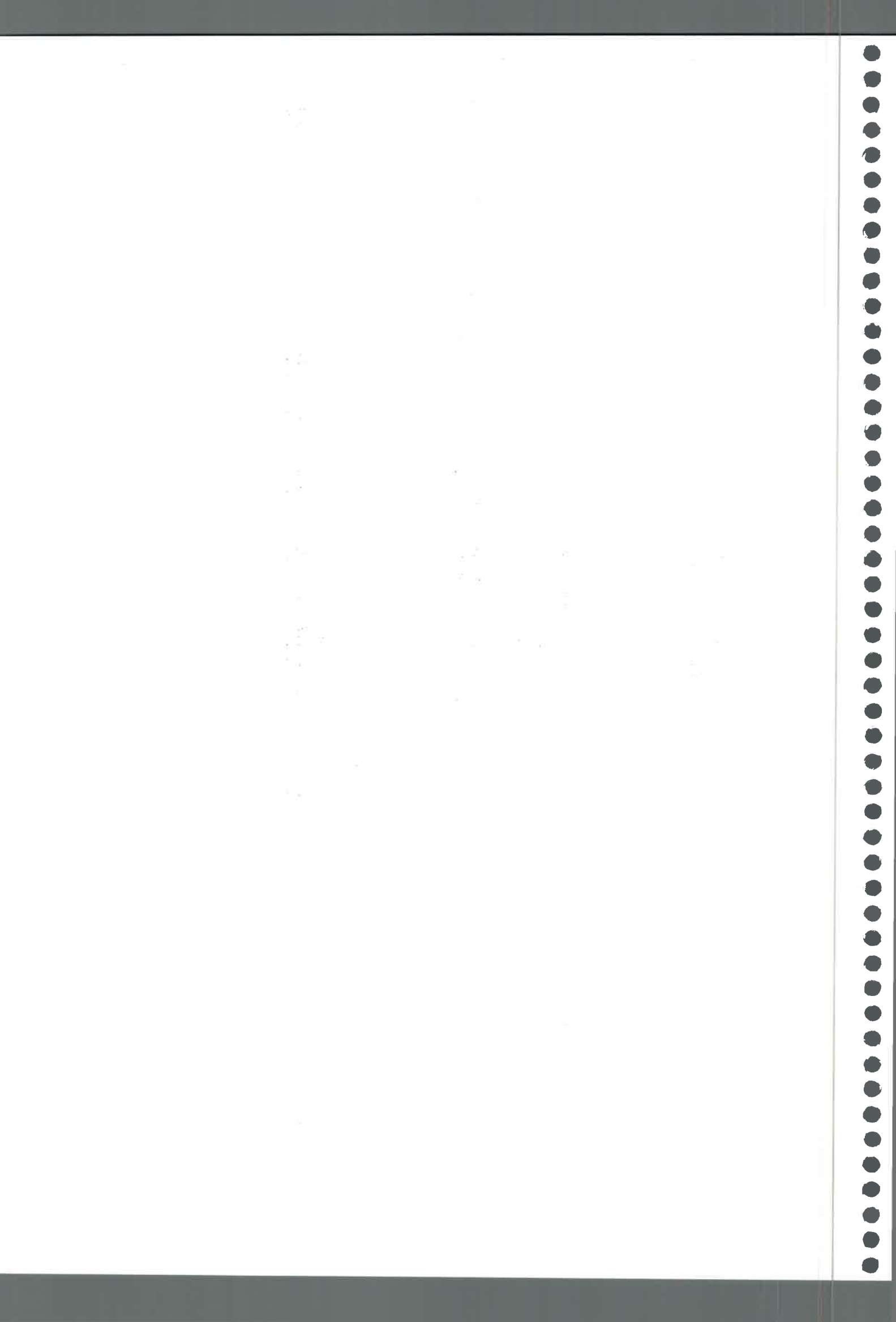
A lo largo de esta década se conectan a Internet las primeras redes europeas y también japonesas, con lo que la red ya es de ámbito verdaderamente mundial.

A finales de los ochenta se producen grandes cambios, aparecen los primeros "crackers"⁸ y "hackers"⁹, aparecen los primeros virus "gusano", la agencia ARPA se retira de la red y sobre todo aparece la World Wide Web (la Telaraña Global). Fue Tim Berners-Lee quien, trabajando en el CERN (Centre Européen de Recherche Nucléaire - Ginebra, Suiza) junto con Rober Cailliau inventó el protocolo de transmisión http y el lenguaje HTML en que se basa la "Web".

En 1993 aparece "Mosaic", el primer navegador.

⁸ "Pirata de la red con malas intenciones, que básicamente se la pasa husmeando lugares ajenos para obtener información confidencial de determinadas compañías, principalmente robo electrónico de capital a los cuenta habientes de los bancos". Definición obtenida en la página www.microsiervos.com.

⁹ "Persona que aprecia el verdadero valor de la programación, que programa creativamente con entusiasmo y rapidez, es una persona que generalmente busca hasta el más mínimo detalle de los lenguajes de programación con el propósito de explotar al máximo sus capacidades. "Hacker" es cualquier persona con gusto, afecto y habilidad hacia algo". Definición obtenida en la página www.microsiervos.com



El año 1995 empieza la gran expansión de Internet, desde entonces se han superado todas las expectativas. En esta época se produce la aparición de la Internet comercial, las empresas se instalan en la red y se ofrecen todo tipo de servicios “on line”, tiendas, bancos,....

Es en esta época también, cuando aparecen los primeros motores de búsqueda, el lenguaje “Java” se incorpora a los navegadores, y se desarrollan otras tecnologías orientadas a convertir a la red en un mundo multimedia lo más atractivo posible.

Internet

Internet es una red internacional o de computadoras interconectadas, que permite comunicarse entre sí a decenas de millones de personas, así como acceder a una inmensa cantidad de información de todo el mundo.

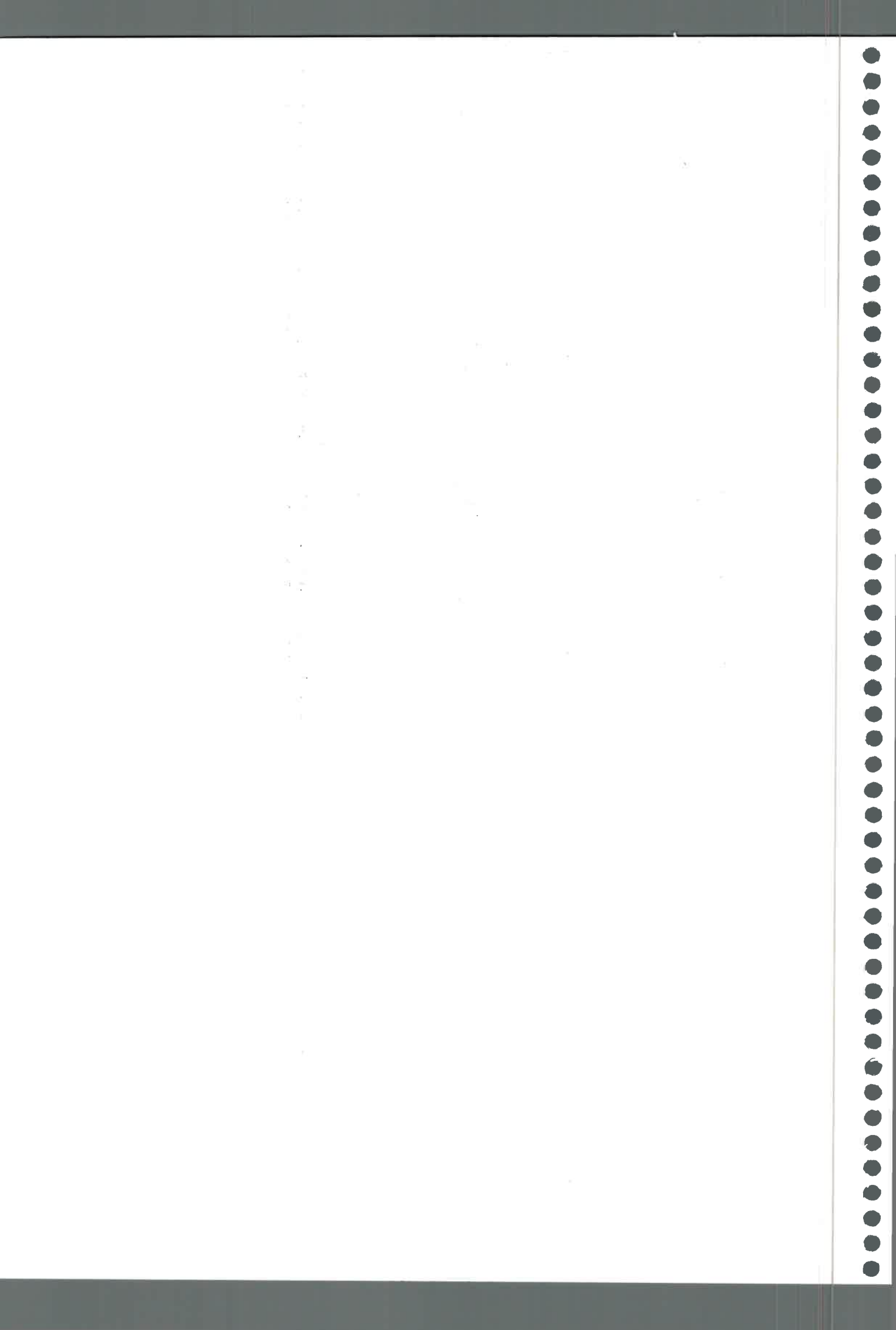
Algunas características relevantes de la misma son¹⁰:

- Es una red abierta, ya que cualquiera puede acceder a ella.
- Es interactiva, ya que el usuario genera datos, navega y establece relaciones.
- Es internacional, puesto que permite trascender las barreras nacionales.
- Hay multiplicidad de operadores
- Carece de un centro que pueda ser denominado autoridad, opera descentralizadamente y construye el orden a partir de las reglas del caos.
- Genera sus propias reglas sobre la base de la costumbre.
- Muestra una aceleración del tiempo histórico.
- Permite la comunicación en tiempo real y una desterritorialización en las relaciones jurídicas.
- Disminuye en forma drástica los costos de transacción.

La tecnología digital produce una desestructuración en conceptos como el espacio, el tiempo o la diferencia entre público y privado que trajo como consecuencia un cambio no solo en la forma de pensar sino en la de realizar las cosas.

Los principales cambios conceptuales que se han generado son:

¹⁰ Lorenzetti, Ricardo. Comercio Electrónico. Citado en referencia 1.



1. Espacio virtual y desterritorialización.

Existe un nuevo espacio, el cibernético o ciberespacio, distinto del espacio físico, caracterizado por su maleabilidad, ya que cualquiera puede definir códigos e interactuar en él.

El ciberespacio es autónomo en el sentido de que funciona según las reglas de un sistema autorreferente. Es posorgánico, ya que no está formado por átomos ni sigue las reglas de funcionamiento y localización del mundo orgánico: se trata de bits¹¹. Tiene una naturaleza no territorial, un espacio movimiento, en el cual todo cambia respecto de todo, por lo que el espacio virtual no es asimilable al espacio real porque no está fijo, no es localizable como por ejemplo por el tacto.

Este espacio no tiene características solamente pasivas, sino activas, en el sentido de que influye sobre los demás sistemas. Produce efectos de desterritorialización y descentralización, porque no hay una relación centro periferia, no conoce jerarquías, y sobre todo no hay una autoridad central. Esto afecta las categorías como la de original-copia, lector-autor, productor consumidor, ya que al cambiar el espacio, cambian los roles.

Es un espacio del anonimato, donde el individuo ingresa sin que interese su historia individual ni sus características y donde prolifera el simulacro de la identidad, caracterizados por la diferencia: clubes, grupos, subgrupos reunidos alrededor de intereses específicos.

Es un espacio que no pareciera tener las características esenciales para definirse como tal. En la tradición se entiende por espacio como "continente de todos los objetos sensibles que existen"¹², pero en este caso no hay continente ni objeto sensible. El espacio tiene límites, que no pareciera existir en el espacio virtual: no reconoce límites geográficos porque ignora a los gobiernos.

¹¹ "Unidad básica de información que puede tomar los dos valores de uno o cero, utilizada en la numeración binaria". Enciclopedia Salvat. Tomo 2. Ed. Salvat Editores S.A. Barcelona 1978

¹² Definición de la Real Academia Española

2. El tiempo virtual.

Una de las características actuales es la aceleración del tiempo histórico. Este fenómeno hace que el presente se torne omnipresente¹³ y que la dimensión del pasado o del futuro se adelgacen.

Actualmente la tecnología permite la comunicación instantánea con cualquier parte del mundo, sin necesidad de consumir recurso escaso como es el tiempo.

El tiempo virtual, al igual que el espacio, se divorció de las categorías naturales que configuran el tiempo real. El día y la noche definieron el tiempo para el trabajo y el descanso, pero ahora se trabaja en lugares cerrados, frente a computadoras, sin que importe si es de día o de noche. Esto ha generado el surgimiento del tiempo individual, reduciendo los vínculos físicos.

3. El domicilio privado.

Las relaciones jurídicas efectuadas por medios electrónicos pueden plantear serios problemas para determinar dónde se realizan.

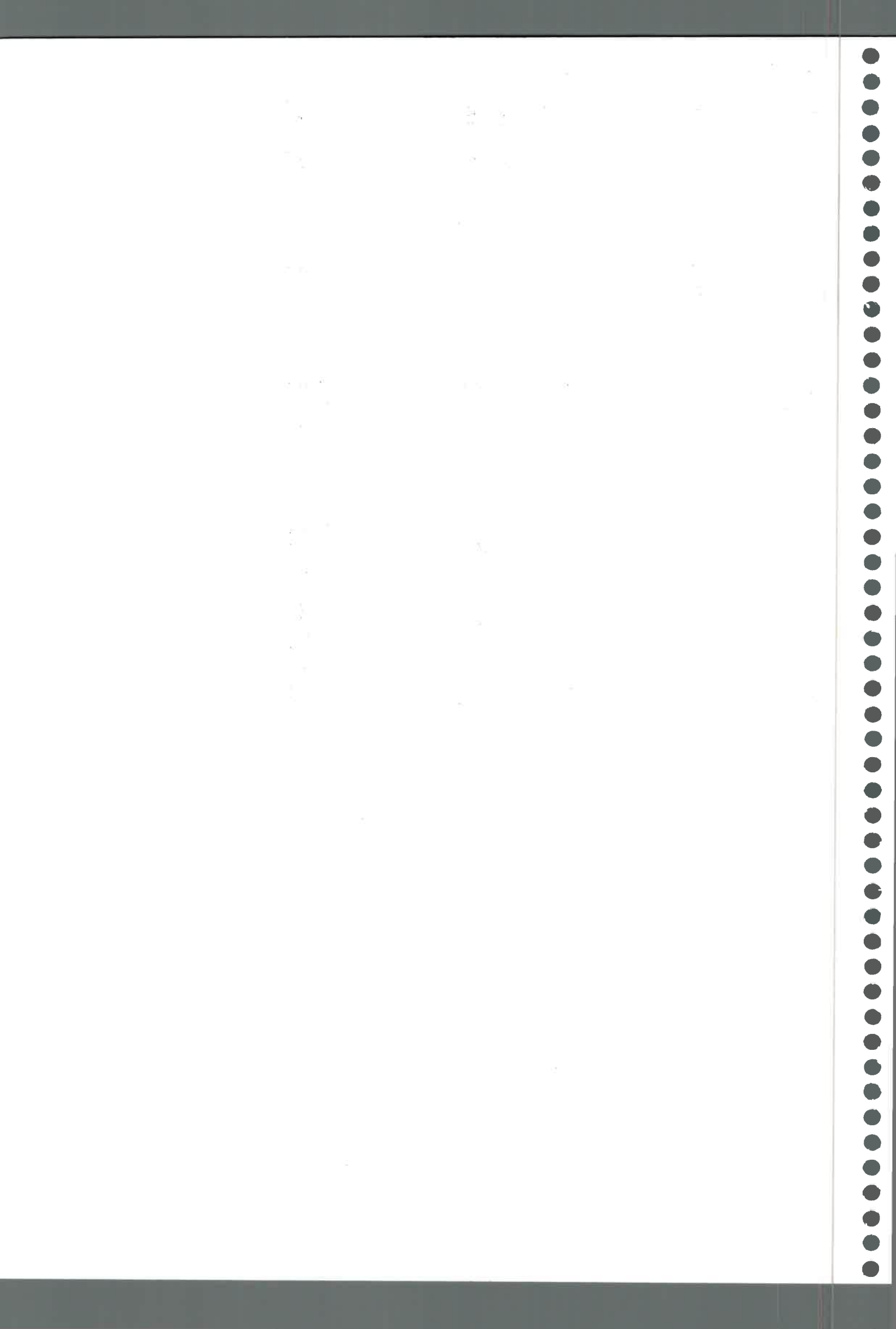
En el campo del consumo, el usuario de Internet puede emitir declaraciones de voluntad desde una computadora ubicado en un sitio diferente de su lugar de residencia o trabajo. También se pueden celebrar contratos en forma instantánea entre sujetos que están en lugares distantes.

Lo que ha generado la necesidad de declarar que lo que realmente interesa para calificar un vínculo como celebrado a distancia no es el espacio sino el tiempo.

4. Tecnología global frente a las barreras nacionales.

La evolución de las tecnologías de la comunicación muestra un creciente ascenso hacia un status global, que fue incipiente con el surgimiento del correo, aumentó con el teléfono y la televisión y alcanza un estadio superior con Internet, que permite a los sujetos comunicarse entre sí sin que sientan una presencia del Estado nacional y su marco regulatorio.

¹³ “Que está a un tiempo en todas partes”. Nuevo diccionario enciclopédico ilustrado. Ed. Sopena Argentina S.A.



El Estado nacional está unido a la noción del territorio donde se ejerce su jurisdicción. Si una tecnología permite entrar en la jurisdicción estatal sin pasar por las barreras establecidas para el espacio físico puede ocasionar problemas respecto a que los individuos pueden contratar la venta o el uso de bienes en forma digital, hacer publicidad, transmitir mensajes de todo tipo, ignorar el sistema jurídico nacional aplicable al territorio donde viven. Pueden violarse el régimen de importación o exportación, las aduanas y los impuestos. Con la compra de bienes digitalizados no existe el contenedor ni la maleta, que son los elementos que se toman en cuenta para el control¹⁴. Fenómenos vinculados con el consumo, servicios bancarios de viajes, turismo, intermediación financiera, software, consultoría, educación, prestaciones de salud, asesoramiento inmobiliario, pueden estar fuera del control del orden público. Temas tan diversos como la prohibición del juego y la pornografía o las barreras de entrada al mercado enfrentan serios desafíos ante la penetración del medio electrónico.

5. Privatización del tiempo y el espacio comunitario.

Estamos frente a una tecnología típicamente posmoderna, en el sentido de que puesta en manos de un sujeto cada vez más individualista, es usada de modo heterogéneo y fractura algunos aspectos importantes de la regulación que se basa en presupuestos comunitarios.

En este contexto reinan el pluralismo y la diferencia.

Por ejemplo: -La prohibición de trabajar en días feriados, o de noche, son regulaciones que tienen finalidad protectorias de los trabajadores y de ordenamiento social, diferenciando el día y la noche, el trabajo y el ocio, y muchas otras funciones. Pero una persona puede trabajar con una computadora en su casa en días feriados, de noche, con lluvia o nieve, y con horarios continuos que ella misma administra, ya que sólo le reclaman objetivos y resultados. -Una persona puede jugar en un casino virtual, haciéndolo desde un país o región donde está prohibida la actividad del juego. -Un operador de bolsa puede comprar acciones en países de otros usos horarios; un niño puede visitar una biblioteca que está cerrada para el público que concurre físicamente.

¹⁴ Greco. Marco Aurelio. Internet e direito. Ed. Dialética. San Pablo. 2000

La influencia de Internet

1. La libertad.

Muchos sostienen que Internet aumenta el poder decisorio del individuo aislado, y ello significa un correlativo incremento de su libertad.

Esta afirmación es cierta desde la perspectiva de la libertad de expresión, ya que el cibernauta puede expresarse, comunicarse, interactuar sobre cualquier tema que le interese, con una multiplicidad de sujetos en todo el mundo

También es importante examinar la contracara de Internet, en cuanto instrumento lesivo de la libertad de los individuos.

La red brinda una apariencia libertaria en el sentido de que a nadie le interesa quién es, si es rico o pobre, si pertenece al primer mundo, al segundo o al tercero; tampoco está a las restricciones de la raza o de la religión, que son discriminatorias en el mundo real¹⁵.

El juego y la simulación son característicos en amplios sectores de la red, siendo el anonimato promovido bajo el paraguas de la libertad de expresión.

Sin embargo, también se observa que el individuo que navega permanentemente e interactúa con una multiplicidad de sujetos, está lejos de alcanzar la plenitud.

La capacidad del usuario de controlar por sí mismo se ve muy limitada por algunas características de la red. Los procesos de identificación en el mundo real son diferentes a los que acostumbramos a utilizar: si uno entra a un negocio, existen exigencias municipales que regulan su apertura, marcas registradas, elementos físicos, lo que da una cierta seguridad. En Internet muchas veces uno se pregunta si lo que se presenta como tal o cual negocio como un banco o una compañía de turismo, lo es realmente. La red diluye la potencialidad de los procesos de identificación y autoría.

La libertad de elegir existe, pero también se incrementa la concentración, y la diferencia de poderío es cada vez más notoria. La estandarización es ventajosa y necesaria, pero provee una base para que grandes grupos establezcan monopolios en materia de hardware, software y comunicaciones¹⁶.

El individuo puede mantener su privacidad, pero la circulación del dato y su difusión es extremadamente peligrosa.

¹⁵ Amato Mangiameli. Diritto e cyberspace. Giappichelli. Torino. 2000

¹⁶ Lorenzetti, Ricardo. Comercio Electrónico. Citado en referencia 1.

En el plano macrosocial, la tecnología digital introduce bajísimos costos de transacciones, en una variedad de campos, lo que genera cambios a nivel coyuntural e institucional. Cambian el trabajo, la posesión de la riqueza y del derecho, proliferando la inseguridad.

2. La privacidad.

Internet debilita los límites del hogar como espacio privado.

La radio, el correo, la televisión invadieron el hogar, pero Internet lo hace de una manera superior, dado que un individuo o una familia pueden trabajar, comprar e incluso votar sin salir de su casa. De ese modo, los usuarios aparecen conectados desde la intimidad, permitiendo a que los oferentes lleguen con sus ofertas directamente a la casa del consumidor.

3. Los costos.

La tecnología digital y, especialmente, Internet tienen un tremendo impacto en la disminución de los costos de búsqueda y celebración de acuerdos, lo cual explica su enorme y rápida difusión en una escala global.

El uso de la red permite bajar sustancialmente numerosos costos de identificación de potenciales clientes y de los usuarios entre sí, porque, en el aspecto técnico la comunicación es instantánea, global, llega a los hogares, permite acceder a cualquier tipo de sujeto sin distinción de edad, raza, sexo o nacionalidad, facilita la segmentación de productos y tiene un enorme potencial en cuanto a la recolección y utilización de datos de todo tipo. Desde la perspectiva económica, los costos comparativos de la comunicación por Internet son más bajos que los de cualquier otra tecnología existente.

Los costos de celebración de vínculos también disminuyen. En el ámbito de la contratación empresarial, la negociación puede hacerse en tiempo real; puede ser más acelerada y automática cuando hay intercambio electrónico de datos con redes cerradas. En las relaciones de consumo, la publicidad llega al hogar del consumidor, en las páginas se instalan las condiciones generales de contratación, y la aceptación se puede hacer mediante un simple clic en el mouse. En muchos sectores hay un impacto creciente del documento electrónico y la firma digital, porque permiten eliminar

grandes volúmenes de papeles y archivos, redimensionando el concepto de administración. En otras áreas, como la bancaria, la bolsa y el sector financiero en general, la aparición del dinero electrónico, las transferencias electrónicas y la información on line reformulan completamente los modelos organizativos. En el plano del consumo, Internet aumenta las posibilidades de interactuar con otras personas, de elegir productos y servicios en un rango cada vez más amplio, de obtener algunas categorías de bienes personalizados y de disminuir el tiempo de la elección, todo lo que reduce drásticamente los costos de transacción en beneficio del consumidor.

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

CAPÍTULO II

Economía digital

Producto de la transformación que ha generado la tecnología digital, la conceptualización de la economía ha cambiado de actores y de escenario. Tres de cada diez personas en el mundo tienen acceso directo e indirecto a Internet, generando que el mercado (lugar donde concurren compradores y vendedores), se transforma en el ciberespacio, las necesidades tradicionales continúan existiendo dentro del ciberespacio, los ofertantes y demandantes se convierten en cibernautas, y el desarrollo del comercio y sus transacciones se realizan de forma digital sin papeles.

Una docena de temas superpuestos que diferencian la nueva economía de la antigua surgen en estos momentos. Al poder comprenderlas tendremos conciencia de la preconcepción requerida para poder dar un vuelco a los actuales negocios y lograr muy pronto el éxito deseado¹⁷.

1. Conocimiento.- Para surgir en la economía actual es básico tener conocimiento sobre los productos, bienes y servicios que ofrecemos como productores, o que requerimos como demandantes, la economía actual está gobernada por el conocimiento.

La tecnología de la información permite la generación de una economía gobernada por el conocimiento, a pesar del surgimiento de la inteligencia artificial y otras “tecnologías del conocimiento”, este último es creado por los seres humanos y por quienes desean seguir avanzando en la búsqueda de nuevas comprensiones para el ser humano. El contenido de conocimiento de los productos y servicios está creciendo en forma significativa a medida que las ideas del consumidor, la información y la tecnología se convierten en parte de los productos. Un claro ejemplo lo constituyen la nueva gama de productos inteligentes, los que desde hace varios años han revolucionado todos los aspectos de la sociedad.

En una economía basada, en el cerebro no el músculo, se evoluciona hacia una economía fundamentada en la inteligencia y en el conocimiento. En la nueva economía,

¹⁷ Huayamave Betancourt, Xavier. La economía digital. 2000. Obterido de la página web www.monografias.com.

los activos claves de la organización son intelectuales y se concentran en el trabajador del conocimiento. El conocimiento no es sencillamente otro recurso paralelo a factores tradicionales de producción como mano de obra, capital y propiedades. Para varios entendidos en la descripción de las fortalezas de la nueva economía, el trabajador del conocimiento de cualquier organización es el mayor y único activo. Es muy cierto que el capital es un activo clave para cualquier negocio a emprender, pero ciertamente muy fugaz. En la economía actual, el capital estará cada vez más en función del conocimiento.

2. Digitalización.- A través de la historia, las revoluciones generadas en los recursos naturales han posibilitado un nuevo paradigma en herramientas (hierro, bronce, acero), que condujeron a nuevos modos de creación de riqueza y desarrollo social. La nueva era podría denominarse apropiadamente la era de la arena. Los acontecimientos en el comercio, transacciones de negocios, comunicaciones humanas y penetraciones de la ciencia se reducen a cargas en partículas de silicio o recorridos a través de fibras de vidrio, ambos elementos derivados de la arena.

Toda la información se puede representar ya sea con un "1" o con un "0", lo que constituye el principio fundamental del sistema binario, que fue el empleado en todos los sistemas de información al inicio de la revolución computacional, con el paso del tiempo se aplicó la digitalización más allá de las cantidades y las letras, y fue posible utilizar los bits para representar cada vez más tipos de información, como gráficas y fotografías.

En la antigua economía, la información era análoga o física, las personas se comunicaban al desplazar sus cuerpos físicos en un salón de reuniones, hablar a través de una línea telefónica análoga, transmitir señales de televisión análogas, enviar cartas, mostrar películas del almacén fotográfico local, intercambiar efectivo y cheques, etc.

En la nueva economía, la información se halla en medios digitales: bits. Cuando es digitalizada y comunicada a través de redes digitales, se abre un nuevo mundo de posibilidades. Vastas cantidades de información se pueden concentrar o comprimir y transmitir a la velocidad de la luz, tomando en consideración que gran parte de esta información puede ser de mejor calidad que las de transmisiones físicas o análogas. Además cuando se crean documentos Multimedia¹⁸, que incluyen medios basados en el

¹⁸ "Información digitalizada que combina texto, gráficos, imagen fija y en movimiento, así como sonidos". Definición obtenida de la página www.definiciones.org

tiempo como el audio y el video, estos pueden estar disponibles en forma instantánea en cualquier lugar del planeta, y pueden tener mejores resultados e impacto en la mayoría de los aspectos de los negocios y la vida personal de los seres humanos.

3. Virtualización.- A medida que la información cambie de analógica a digital, los elementos físicos se tornarán virtuales, cambiando el metabolismo de la economía, los tipos de instituciones y relaciones posibles, y la naturaleza de la actividad económica en sí misma.

En la nueva economía, existen para nombrar unos pocos, los siguientes ejemplos:

Extranjeros virtuales. Son las personas que trabajan y participan en la economía de un país, quienes físicamente están localizadas en algún lugar diferente; por ejemplo, programadores o diseñadores gráficos que trabajan a miles de kilómetros de la compañía que los ha contratado y que envían sus trabajos a través de la Internet.

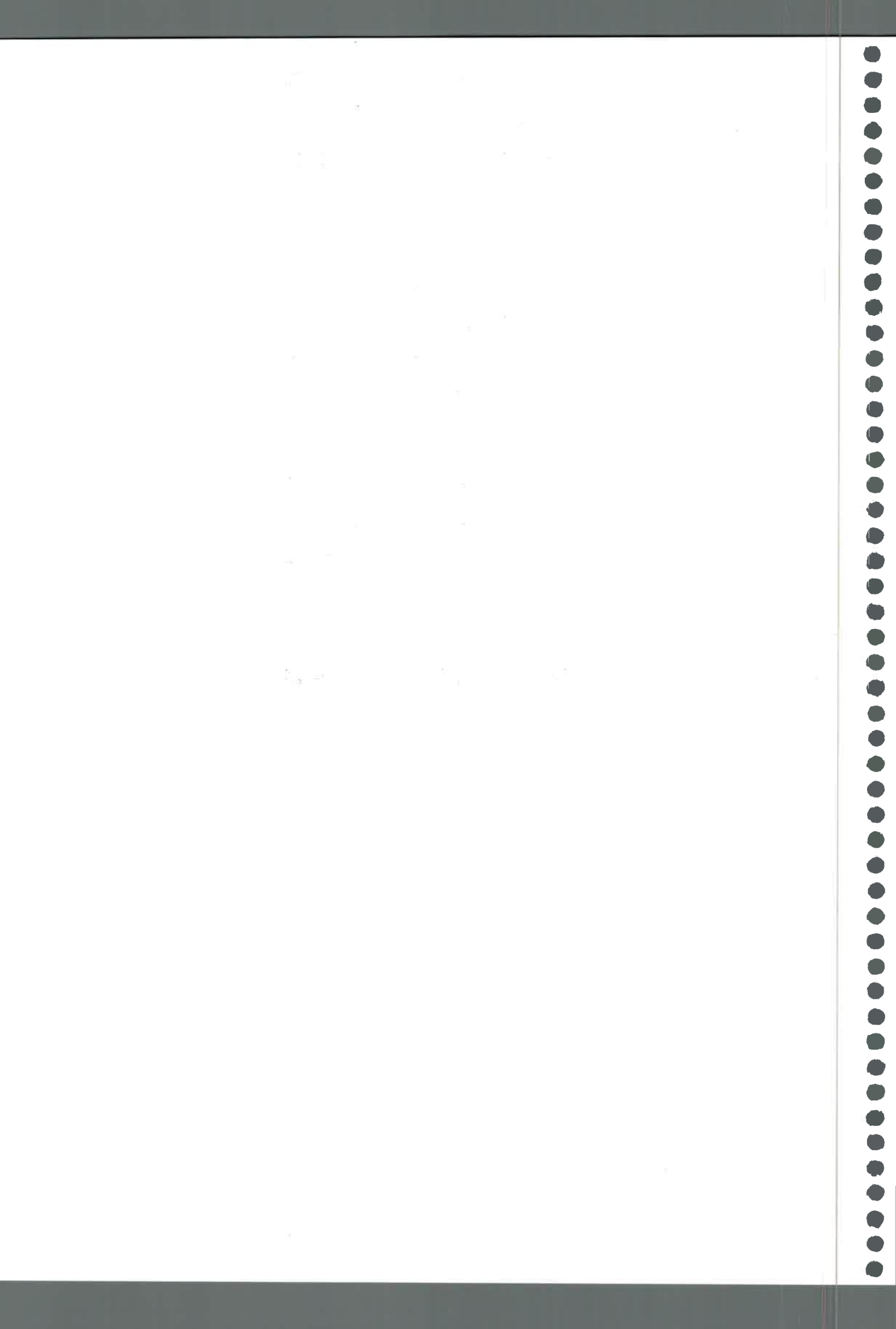
Incubadoras de negocios. Son todas las herramientas que brinda una compañía en la red, para que el interesado pueda crear y diseñar negocios catalogados como "proyectos", y que necesitan de ayuda externa (logística, financiera, tecnológica, etc.) para poder concretarse.

Centro comercial virtual. Un ambiente en la red en el cual las cosas o los artículos preferidos se pueden hallar, como oferta virtual, físicamente no se encuentra allí pero sirve de enlace entre compradores y proveedores.

Aldea virtual. Es la agrupación de individuos, independientes en cuanto a la localización, que comparten un amplio conjunto de intereses comunes objetivos y subjetivos. Se extiende a la vida en la aldea, su calle principal, plaza e inclusive al bufón del lugar. En la mayoría de estas aldeas existen reglamentos que rigen desde su compostura, hasta el sexo virtual.

4. Molecularización.- La nueva economía es molecular¹⁹, la antigua corporación está en proceso de desagregación, siendo reemplazadas por moléculas dinámicas y multitudes de individuos y entidades que conforman la base de la actividad económica. La organización no desaparece, pero si "evoluciona". Lo masivo se convierte en molecular en todos los aspectos de la vida económica y social. La jerarquía y la economía industriales están dando lugar a las estructuras económicas y organizaciones moleculares, la analogía es útil para comprender a la nueva economía, puesto que la

¹⁹ "Molécula: mínima porción de un compuesto que mantiene las características de la especie". Enciclopedia Salvat. Tomo 8 Ed. Salvat Editores S.A. 1978



nueva empresa tiene una estructura molecular fundamentada en el individuo. El trabajador del conocimiento funciona como una unidad de negocios de una entidad.

Los trabajadores motivados, autodidactas, con espíritu empresarial, con poder y con el sentido de cooperación a través de nuevas herramientas, aplican su conocimiento y creatividad para crear valor. Las condiciones pueden garantizar una estructura sólida que una fuertemente las moléculas. Por ejemplo, los medios masivos de comunicación se convertirán en medios moleculares, a través de los cuales los lectores, oyentes y televidentes serán clientes que podrán tener acceso e interactuarán con millones de "canales".

5. Integración/ Interconexión en red.- La nueva economía es una economía en red, integra moléculas en conjuntos que se interconectan con otros para la creación de bienestar. El nuevo paradigma en la creación de bienestar es posible gracias a las redes computacionales que son digitales, no analógicas, y debido al cambio en el estilo de trabajo en red interconectada en contraste con la conexión del computador tipo anfitrión, redes jerárquicas de las antiguas redes par a par basadas en el modelo de Internet. A medida que aumenta el ancho de banda de dichas redes para lograr una multimedia total (integración de datos, texto, audio, imagen y video), crecen dramáticamente las oportunidades para estas nuevas estructuras institucionales.

Las redes de la nueva tecnología permiten a pequeñas compañías superar las principales ventajas (economías de escala y acceso a los recursos) de las grandes firmas. Al mismo tiempo, estas pequeñas empresas no se ven agobiadas por las principales desventajas percibidas en las grandes organizaciones: burocracia agonizante, jerarquías sofocantes e incapacidad para cambiar. A medida que las grandes empresas entran en desagregación, se convierten en pequeñas moléculas que unidas pueden funcionar bien, ganando en ventajas de agilidad, autonomía y flexibilidad.

La empresa interconectada en la red se comportará como la Internet en la que todos pueden participar y el esfuerzo total es mayor que la suma del esfuerzo de las partes, todo esto, sumado a la gran infraestructura que cada gobierno por su parte deberá desarrollar un sistema nacional de información, el cual será el servicio público del siglo XXI, una autopista de banda amplia para una economía de banda ancha y gran capacidad. Y cada organización necesita conectarse a este servicio público con una infraestructura empresarial de información. La nueva infraestructura cambiará la actividad económica en forma tan significativa como lo hizo la electrificación. Así

como los negocios y la creación de bienestar no serían actualmente concebibles sin la electrificación, de igual manera, la nueva economía sería imposible sin el poder de la información.

6. Desintermediación.- Las funciones de intermediación conocidas entre los productores y consumidores se están eliminando a través de redes digitales. Las empresas, funciones y personas intermediarias necesitan subir en la cadena alimenticia para crear un nuevo valor, o enfrentarán la desintermediación. Si la compañía tiene en su núcleo agentes, mayoristas, distribuidores, minoristas, corredores de bolsa o gerentes de nivel medio, es el momento de realizar serios movimientos estratégicos. Los músicos y sus producciones no necesitarán disqueras, agencias de venta minorista ni medios de difusión cuando su música se convierta en una base de entrada de datos en la red.

Los fabricantes podrían utilizar la nueva infraestructura para vender a través de la red, eliminando en consecuencia los canales minoristas intermediarios.

Otro candidato para el proceso de desintermediación es el Gobierno. Sus clientes (el público), deben hacer una larga fila en quince lugares diferentes para tratar con quince organismos públicos diferentes, cada una con personal, subcontratistas, costos, y todas en gran medida con un alto nivel de inseguridad, maltrato, y poca eficiencia en el servicio a sus usuarios, a este nivel se necesita de mucho licerazgo por parte del gobierno para crear una sola ventana (una sola cara), a la que se tendría acceso a través de la autopista de la información desde el hogar, computadoras públicas, sitio de trabajo o cualquier otro tipo de dispositivo de información. Los usuarios podrían interactuar con servicios basados en el computador cuando sean adecuados o interactuar con seres humanos (audio y video) cuando la consulta sea más especializada.

7. Convergencia.- Mientras en la antigua economía, la industria automotriz era el sector clave, en la nueva el sector predominante son los nuevos medios de comunicación, los cuales son producto de la convergencia de las industrias de computación, comunicaciones y contenido. El hardware y el ancho de banda de las comunicaciones se están convirtiendo en productos populares. Las utilidades en el nuevo sector se desplazan al contenido debido a que es ahí donde se crea el valor para los clientes, no en las cajas o en las transmisiones. Muchas de las compañías de contenido —empresas de entretenimiento, redes de transmisión y editores— se encuentran rezagadas ante la resistencia de los antiguos paradigmas. Las empresas más exitosas son

1000

1000



aquellas con experiencia en software, servicios, contenido basado en la computación y telecomunicaciones digitales.

La convergencia se convierte en base de todos los sectores. Los nuevos medios ya están comenzando a transformar las artes, la forma como se dirige la investigación científica y como se proporciona la educación. Están en el umbral de la transformación de la firma como se conoce y están cambiando la manera como los individuos realizan negocios, trabajan, juegan, viven e incluso piensan.

8. Innovación.- La innovación básicamente busca que la constante evolución del conocimiento haga obsoletas las ideas, diseños, estructuras, metas y avances del ser humano.

Un impulsor clave en la nueva economía es la innovación, la cual constituye un compromiso con la continua renovación de productos, sistemas, procesos, mercadotecnia y personal.

En una empresa de innovación, los ciclos de vida del producto colapsan. Los fabricantes de automotores japoneses trabajan en un ciclo de vida de dos años, y los fabricantes japoneses de productos electrónicos de consumo estiman un ciclo de tres meses. Algunos productos financieros en determinados mercados tienen un ciclo de vida de unas pocas horas, para entonces la competencia se habrá adelantado. La mayoría de las empresas de mediana o gran magnitud en Norteamérica introduce un nuevo producto diariamente. Para el año 2.000, Sony introdujo 6.500 nuevos productos.

Para ratificar esta aseveración incluimos un comentario hecho por Nathan Myhrvold quien manifiesta: "No importa cuán bueno sea su producto, usted se encuentra únicamente a 18 meses del fracaso"²⁰.

En la economía de innovación, la imaginación humana, es la principal fuente de valor. El desafío crítico para cualquier compañía en la economía digital consiste en generar un entorno donde se premie, recompense y estimule la innovación.

Cada país necesita sitios de trabajo innovadores y organizaciones que estimulen la creatividad. Lo que se necesita son sistemas educativos que enseñen y motiven a los estudiantes a aprender y a ser creativos, en vez de repetir información. Los gobiernos y las estructuras reguladoras deben ayudar a liberar el espíritu humano para la invención y la creación, no actuar como freno burocrático en el proceso de cambio y desarrollo.

²⁰ Huayamave Xavier. "La economía digital". Citado en referencia 17.

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

100

Un productor o vendedor de bienes y servicios debe innovar más allá de lo que los mercados puedan imaginar. Deben comprender las necesidades de los clientes y constar con una organización de una profunda y penetrante comprensión de las tecnologías emergentes. Basada en un ambiente donde no se penalice el hecho de asumir riesgos, donde la creatividad pueda florecer y la imaginación pueda volar.

9. Pro consumidores.- A medida que la producción masiva es remplazada por la individualización en masa, los productores deben crear bienes específicos que reflejen las necesidades y gustos de los consumidores individuales. En la nueva economía, los consumidores se involucran en el proceso real de producción.

En la antigua economía, los usuarios observaban las noticias en las noches; en la nueva economía, un televidente diseñará una transmisión individualizada de noticias al destacar los diez temas de mayor interés y al determinar las fuentes de noticias, comentarios editoriales y estilos gráficos preferidos

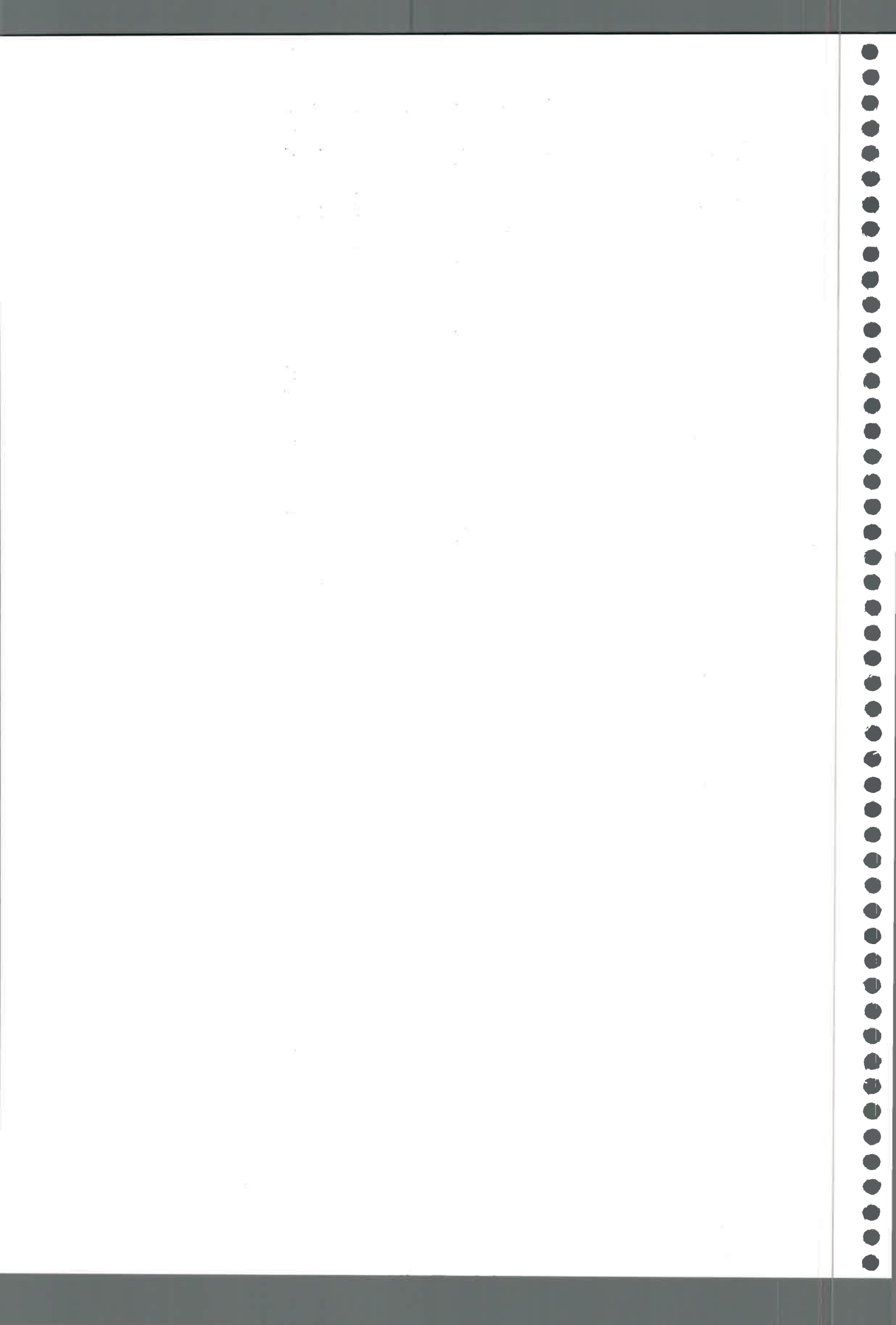
Cada consumidor en la autopista de la información se convierte en un productor al crear y enviar mensajes a un colega, al contribuir en un grupo de análisis de la cartelera, al modificar el final de una película, al hacer pruebas de conducción de un automóvil virtual o al visualizar el cerebro de un paciente en cualquier punto del planeta. A medida que aumenta el contenido de información y conocimiento de los productos y servicios, las organizaciones pasarán de ser solo consumidores de información y tecnología, a convertirse en productores de infotecnología.

10. Inmediatez.- En una economía basada en bits, la inmediatez se convierte en un impulsor y variable clave en la actividad económica y el éxito de las empresas.

Los ciclos de vida de los productos se están reduciendo. En 1990, los automóviles necesitaban de seis años para pasar del concepto a la producción. Actualmente, se emplean dos años. Para las nuevas corporaciones es casi un hecho que la mayor parte de sus ingresos globales en un año provienen de la venta de artículos que el año anterior no existían, es decir que el factor de novedad unido a la rapidez con la que se fabrica o se construye, constituye un poderoso aliado estratégico.

Para la antigua economía el descubrimiento de algo nuevo, o un nuevo invento (como la cámara Polaroid, o la xerografía); aseguraban una corriente de ingresos durante décadas. En nuestros días, los productos eléctricos para el consumo tienen un ciclo de vida típico de dos meses.

La nueva empresa es una empresa de tiempo real, la cual continua e inmediatamente se ajusta a las cambiantes condiciones de los negocios a través de la



inmediatez en la información. Los pedidos de los clientes llegan en forma electrónica y se procesan de manera instantánea; las facturas correspondientes se envían por medios electrónicos y se actualizan las bases de datos. Las empresas buscan “competir en tiempo” de manera efectiva.

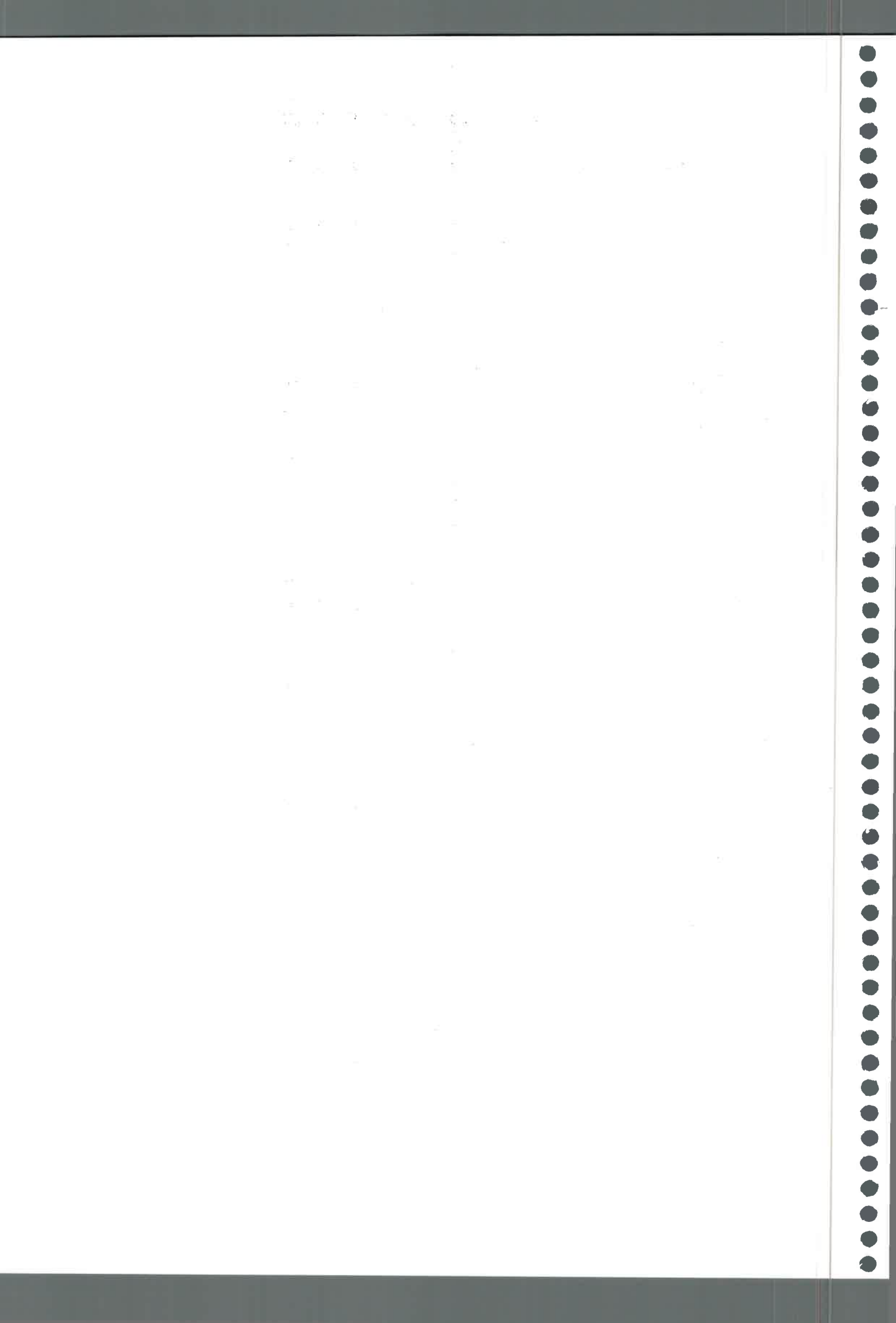
El intercambio electrónico de datos se constituye en un poderoso ejemplo, de la inmediatez de la información. Es justamente la primera señal en una oleada de comercio electrónico que desplazará la evolución de los negocios hacia el tiempo real y al hacerlo de esta manera modificará para siempre las relaciones entre las compañías.

11. Globalización.- Así como el mundo geopolítico bipolar se ha desintegrado, dando paso a un ambiente global nuevo, dinámico y volátil, las barreras económicas también se están derrumbando. Este fenómeno se relaciona con el surgimiento de la nueva economía. No existe conocimiento doméstico ni internacional. Al convertirse el conocimiento en el recurso clave, sólo existe una economía mundial, aunque la organización individual opere en el escenario nacional, regional o local.

Clientes globales exigen productos globales. El trabajo se globaliza al explotar las ventajas en costos de los factores tradicionales de insumos como la mano de obra y materias primas. Las nuevas regiones y estructuras económicas y políticas (como la Unión Europea) están llevando a la decadencia la importancia del concepto estado-nación.

La globalización es al mismo tiempo causa y efecto. Está impulsada e impulsa la nueva tecnología que posibilita la acción global. Las redes computacionales permiten que las empresas suministren servicios las 24 horas a medida que las solicitudes de los clientes se transfieren de una zona de tiempo a otra sin que el cliente se dé cuenta de que el trabajo se realiza al otro lado del mundo. Las redes posibilitan que las firmas pequeñas colaboren en la obtención de economías de escala. La oficina ya no está en un lugar, está en un sistema global. La tecnología está eliminando el concepto de “espacio” en el lugar de trabajo, el hogar puede ser el sitio donde se encuentre el corazón, pero cada vez más, la oficina está en cualquier parte donde se pueda conectar el cerebro.

En forma similar, la globalización está impulsando la expansión de la tecnología, el mundo geopolítico está abriendo nuevos mercados en todas partes, exigiendo una respuesta global. Los negocios globales necesitan poder vincularse con clientes, proveedores, empleados y socios en todo el mundo, y la mayoría estamos trabajando o pensando convertir alguna “empresa transnacional”, “red de respuestas”, “firma sin



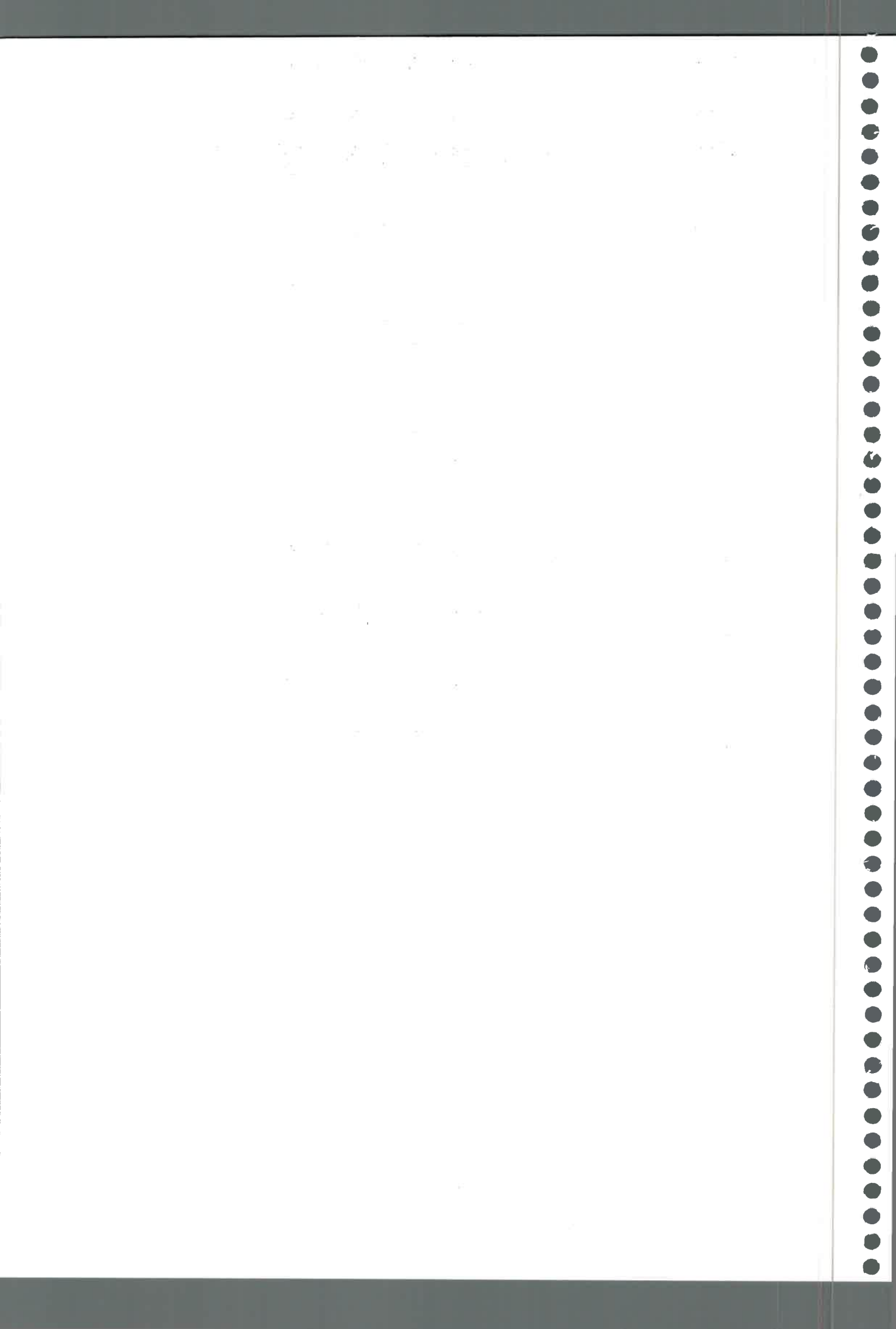
fronteras”, “organización global” o “empresa internacional”; como una manera de globalizar nuestra mente y nuestra visión como empresarios.

12. Discordancia.- En cuanto el hombre se sitúa en las fronteras de la nueva economía, puede observar los comienzos de una nueva economía política que generará profundos planteamientos en torno al poder, la privacidad, el acceso, la igualdad, la calidad de vida laboral, la calidad de vida en general y el futuro del proceso democrático mismo. A medida que los desplazamientos tectónicos²¹ que ocurren en la mayoría de los aspectos de la existencia humana choquen con las viejas culturas, muchos conflictos sociales importantes romperán la configuración de las estructuras e instituciones.

La naturaleza del trabajo y las exigencias de la fuerza laboral en la economía digital son en lo fundamental diferentes. El concepto de mano de obra está experimentando una redefinición radical. Así como el porcentaje de fuerza laboral en la agricultura ha disminuido desde finales del siglo, la cantidad de trabajadores involucrados en la producción de bienes (la antigua economía) ha estado decayendo durante los últimos quince años. La nueva economía genera empleos bien remunerados y de gran valor, pero existe poca movilidad laboral entre la antigua y la nueva. ¿Cómo sucederá esta gran reorganización de la fuerza de la mano de obra y sus habilidades?. La respuesta es que esta gran revolución se logrará únicamente cuando el conocimiento domine en los centros de estudio y aprendizaje de la nueva era, cuando la percepción de la gente se transforme y comprenda cuál es la tendencia actual y hacia dónde camina el mundo actual. Tal como estamos, la tendencia educacional se centrará más hacia las carreras con inclusiones de aprendizaje tecnológico, métodos de desarrollo del conocimiento aplicado a la era digital, sistemas computacionales y desarrollo sistemático de nuevas formas de creación de riqueza, todas que vayan de la mano con la transformación cambiante del mundo moderno.

En la nueva economía, aquellos trabajadores con acceso a la nueva infraestructura pueden participar plenamente en la vida social y comercial. La tendencia de aquellos sin acceso, conocimiento ni motivación es quedarse a la zaga. Si esta situación no se maneja en forma apropiada, se incrementará en forma severa la estratificación social, creando una nueva subclase. Los desposeídos se verán enfrentados a la contradicción entre, por una parte, el espléndido potencial de la nueva tecnología y, por otra, la decadencia en su calidad de vida.

²¹ “Pertenece o relativo a la estructura de la corteza terrestre”. Enciclopedia Salvat. Tomo 12. Ed. Salvat Editores S.A. 1978



CAPÍTULO III

Documento electrónico

Las computadoras son máquinas que realizan operaciones aritmética y lógicas automáticamente, sobre la base de un programa y sin la necesidad de intervención del hombre durante el proceso, a través de pulsos eléctricos.

Como la representación de hechos y actos que ocurren en la realidad puede realizarse de diferentes maneras (verbal, escrita, etc), también puede efectuarse a través de este sistema eléctrico, que lo denominamos digital²².

Es así como la ley 25506 en su artículo 6 define al documento digital como una representación también digital de hechos y actos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo: esto es eléctrico, magnético, óptico, etc. Considerándose además que, a los fines de las exigencias prescriptas por el ordenamiento jurídico, el documento digital satisface el requerimiento de la escritura.

Las principales dificultades que se observan en el estudio de este tema provienen del pensamiento de que el documento está inexorablemente unido a la documentación escrita y que la única evidencia certera de autoría es la firma holográfica²³.

Reglas de autoría histórica

Es una regla admitida y difundida que la relación entre el documento, la escritura y la firma holográfica es un modo confiable de atribución de autoría.

El consenso legislativo, la difusión en las costumbres y la antigüedad de la regla le dan una apariencia de ser absoluta, lo que no es real. Esta regla se extendió en su aplicación en función de la difusión de los presupuestos tecnológicos que la hicieron viable: primero el uso del papel y, posteriormente la imprenta.

²² Fraschetti, Alejandro. La ley de firma digital y las presunciones de autoría e integridad

²³ "Firma holográfica: firma autógrafa de puño y letra". Santos Cifuentes. Elementos del derecho civil. Parte general. Ed Astrea.

Resulta, entonces obvio, que si disminuye el uso del papel y de la imprenta surgirán otras herramientas para dar respuestas a los cambios. Por ello, cuando se utilizan medios electrónicos en lugar del papel, bits en lugar de átomos, algunas reglas deben cambiar.

Aun cuando se admitiera la plena validez del documento escrito y firmado, hubo siempre otras modalidades complementarias. El uso de los testigos, la palabra y el juramento fueron comunes en el derecho romano como modos de acreditar la autoría.

Documento y documentación

Según el diccionario de la real academia española, la palabra documento proviene del latín “documentum” que deriva del verbo “docere” que quiere decir enseñar, hacer, saber, anunciar.

El concepto de enseñar implica también el de mostrar, indicar; y éstos a su vez el de presentar, es decir poner algo en presencia de uno. Cuando ese mostrar se produce a través de otra cosa, estamos ante la representación. De éste modo la figura, imagen o idea sustituye la realidad.

O sea que, el documento, como el testimonio o la confesión, es el resultado de la actividad humana; es decir poner algo en presencia de uno, produciéndose lo que podríamos llamar una “representación”. Es la imagen de la realidad la que se presenta al intelecto a través de los sentidos y en consecuencia, documento es una cosa que sirve para representar a otra. De allí que se concluye que mientras que el acto testimonio o confesión es por sí mismo representativo del hecho testimoniado o confesado, el acto que crea el documento no es representativo del hecho narrado en éste, sino que se limita a crear el vehículo de representación, que es ese documento.

Podríamos decir en términos amplios que debe entenderse por documento a cualquier objeto que contiene una información que narra, hace conocer o representa un hecho, cualquiera sea su naturaleza, su soporte o su continente, su proceso de elaboración o su tipo de firma.²⁴

²⁴ Rolero, Graciela Lilián. Documento electrónico y firma digital. Necesidad de una legislación específica. II Congreso Internacional de Derechos y Garantías en el siglo XXI. Universidad de Bs. As, Abril 2001

El documento tiene dos elementos: a) la docencia, es decir, la capacidad de incorporar y transmitir una declaración de voluntad emanada de un autor y destinada a producir efectos jurídicos sobre su esfera de intereses.; b) la documentación o soporte, que es la forma que adopta esa declaración, es decir, una cosa, como, por ejemplo, un papel o una cinta magnética.

La declaración puede ser a) “corporal”, haciendo referencia al mundo de los átomos; b) “incorporal” o “inmaterial”, o electrónica o digital, haciendo referencia al mundo de los bits.

La expansión de la regla del documento escrito hizo que esta distinción se dejara de percibir.

La generalización de la forma corporal hace que estemos acostumbrados a solucionar fácilmente muchos de los problemas que trae la asignación de autoría, pero que tengamos problemas cuando la documentación es incorporal.

El documento es²⁵:

- un presupuesto de la existencia del contrato, porque cuando la ley impone la forma escrita para acreditarlo, no existe sin esa forma;
- un presupuesto de la eficacia al constituirse en un medio de prueba: porque cuando se requiere la forma escrita, no se puede aportar otra evidencia;
- un presupuesto de la oponibilidad del contrato a los terceros: porque para invocarlo frente a terceros, la ley exige en numerosos casos, forma escrita, fecha cierta o la existencia de un acto público;
- un acto de fijación del contenido de la declaración, porque ésta queda expresada, fijada en la corporalidad.

Todos los problemas que surgen en la contratación electrónica no se relacionan con la declaración de voluntad, sino con el asiento de ésta, es decir, con la mudanza de una documentación “corporal” hacia una “incorporal”.

El problema se reduce notoriamente, no se trata de un nuevo sistema de reglas. De lo que se trata es de garantías, es decir si los bits ofrecen seguridad suficiente para cumplir las funciones descriptas.

²⁵ Lorenzetti, Ricardo. Comercio Electrónico. Citado en referencia 1.

Documento y firma

La relación entre documento y firma parece inmutable, ya que todo documento que no está firmado carece de evidencia clara de autor.

De la palabra documento, también se distingue la palabra “instrumento” (como algo destinado a instruirnos e informarnos del pasado). En la base de la noción de documento está la idea de docencia, en el de instrumento la de prueba.

Mientras que documento es toda representación material destinada e idónea para reproducir una cierta manifestación del pensamiento, el instrumento, es la escritura destinada a constatar una relación jurídica²⁶.

En el Código Civil argentino los instrumentos tienen soporte papel y su finalidad es que la voluntad se exprese por escrito a fin de dar certidumbre y fijeza a las relaciones jurídicas.

Se puede distinguir entre²⁷:

a) Instrumentos públicos, que requiere la presencia de un oficial público, competente y capaz, que actúa sujeto a la ley, según la naturaleza del acto.

b) Instrumentos particulares, que son otorgados por las partes, conjunta o separadamente, firmados o no firmados.

Los instrumentos particulares que llevan la firma del otorgante o de los otorgantes se denominan instrumentos privados.

Entre los instrumentos particulares no firmados podemos mencionar:

- a) Los libros de los comerciantes.
- b) Instrumentos particulares que contengan notas escritas del acreedor.
- c) Instrumentos particulares con impresión digital.
- d) Instrumentos particulares firmados a ruego²⁸.
- e) Billetes de pasajes de transporte (terrestre, aéreo).
- f) Ticks expedidos por cajeros automáticos.
- g) Actos jurídicos celebrados por télex o por fax.
- h) Transferencias electrónicas de fondos.

²⁶ Rolero, Graciela Lilián. Documento electrónico y firma digital. Necesidad de una legislación específica. Citado en referencia 24.

²⁷ Beascoechea de Gánave, Ketty Ruth- Sársfield Novillo, Mario. Instrumentos particulares. Documentos Electrónicos.

²⁸ “Firma a ruego: mandato verbal o tácito, por el cual el mandante que no sabe firmar ruega a un tercero que lo haga por él. Santos Cifuentes. Elementos del derecho civil. Parte general. Ed. Astrea.

- i) Actos realizados mediante cajeros automáticos previa inserción de la tarjeta con banda magnética y alimentación de la máquina con clave numérica personal del titular.

En consecuencia con los avances tecnológicos, se afirma que también constituyen instrumentos particulares no firmados “los impresos, registros visuales o audiovisuales de cosas o hechos y, cualquiera fuese el medio empleado, los registros de pensamientos o información”²⁸.

De esta manera, se entiende por firma el trazo escrito de una manera particular, mediante el cual una persona rubrica sus instrumentos en forma habitual. La firma no es la simple escritura que una persona hace de su nombre o apellido: es el nombre escrito de una manera particular, según el modo habitual seguido por la persona en diversos actos sometidos a esta formalidad²⁹.

En principio este trazo escrito debe corresponder al nombre y apellido del firmante, no siendo relevante que el mismo sea legible o no. Lo que es fundamental es el carácter de habitualidad, es decir que el trazo sea siempre el mismo, sin perjuicio de las alteraciones de detalle que pudieran producirse con el tiempo.

Señala López Olaciregui que “la firma es firma aunque sea ilegible y no es firma aunque sea legible si no corresponde a la habitual forma de suscribir los actos del sujeto jurídico que la estampó”³⁰.

O sea que la regla general es de libertad en la expresión gráfica, y por ello se acepta la validez de la firma que sólo contienen el apellido del otorgante, y aún sus iniciales u otros signos cuando ello constituyere su forma habitual de firmar.

La firma presenta los siguientes caracteres³¹:

- a) Debe ser autográfica, escrita por la mano del otorgante
- b) Habitualidad, debe ser la manera común y habitual de colocar su nombre.
- c) Singularidad, debe ser la manera particular de colocar su nombre. El nombre puede estar colocado de una manera irregular o incompleta, con errores ortográficos, omisiones de letras, falta de rúbrica, con trazos ilegibles, pero si es la manera peculiar que la persona tiene de hacerlo es tenida como una

²⁸ Proyecto de Unificación Legislativa de 1987, art. 978 y Proyecto de reformas del Código Civil de 1992, art. 589.

²⁹ Código Civil Argentino, art. 3633 en concordancia con la nota al art. 3639, último párrafo.

³⁰ Salvat-López Olaciregui. Tratado de derecho civil argentino. Parte General, 1964

³¹ Beascoechea de Gáname, Ketty Ruth- Sársfield Novillo, Mario. Citado en referencia 27.

prolongación de su personalidad y lo irregular de la escritura no vacía la firma.

La inserción de la firma en un instrumento público o privado permite individualizar al sujeto que la suscribe, dado su carácter habitual que implica un trazo particular.

Además de individualizar a quienes intervienen en el acto, la firma inserta en un documento implica la conformidad del firmante con su contenido.

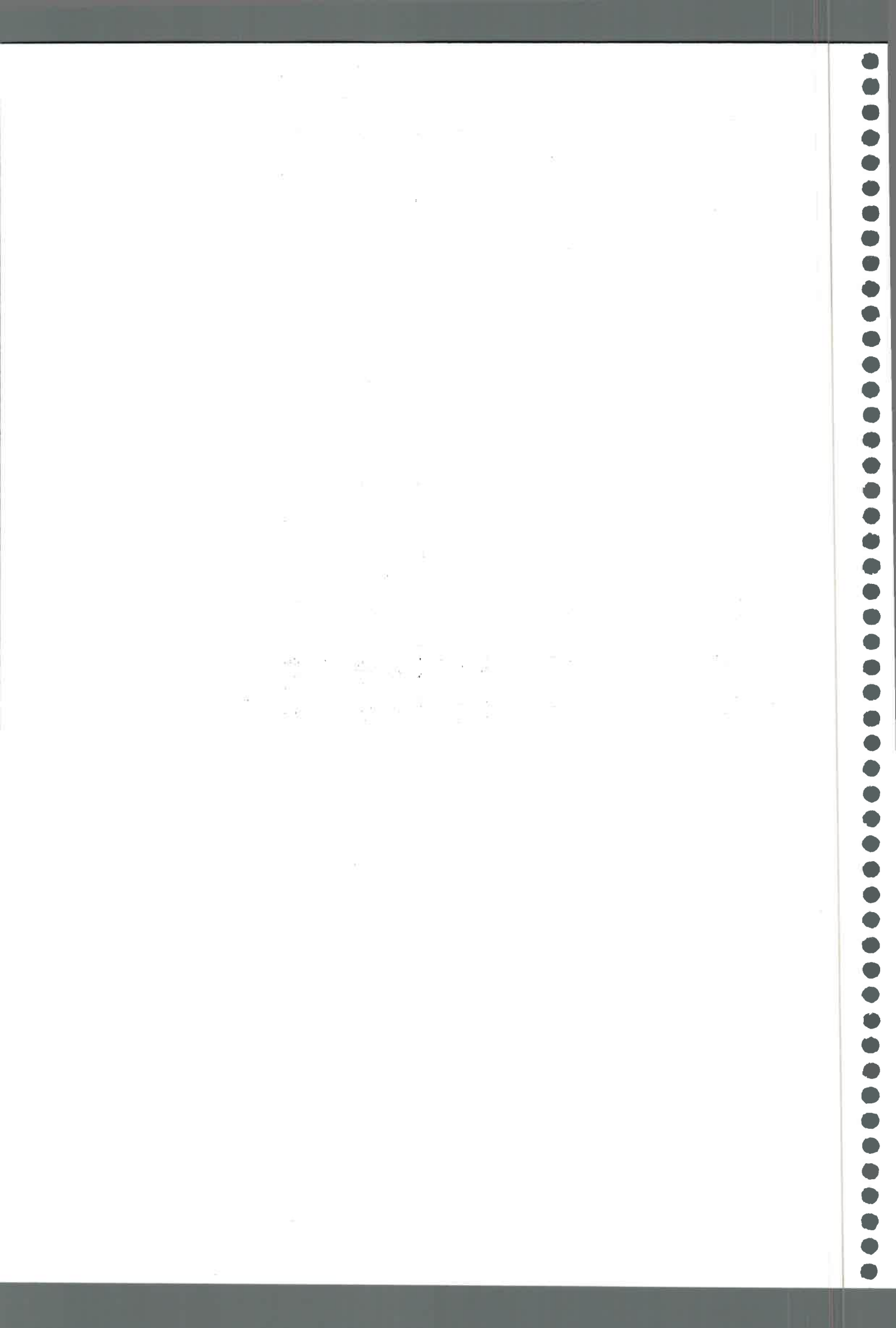
Por ello el artículo 1028 del Código Civil establece que el reconocimiento de la firma implica el del texto suscripto con ella. Lo que la ley ha previsto es una suerte de unión entre el reconocimiento de la firma y el reconocimiento del cuerpo del instrumento y por ello se ha resuelto que la exigencia de la firma como condición esencial del instrumento privado constituye una garantía para los particulares, consistente en que nadie puede juzgar instrumentos en su contra sin la intervención del propio interesado.

En principio, con la firma atribuimos la autoría del documento al o los firmantes, pero se registran casos en que los instrumentos no son necesarios que sean firmados como por ejemplo los boletos de ferrocarril y las entradas a espectáculos públicos, los cuales en realidad constituyen instrumentos particulares no firmados.

Este concepto de firma responde a un esquema tradicional donde el modo de realizarla era la escritura, y la ubicación que debía tener en el documento o instrumento signado era relevante. Sin embargo, cuando el documento es digital, ambas características pierden relevancia, adquiriendo importancia solo su función: identificar al sujeto que lo emite y considerarlo como prueba de la manifestación de su voluntad. Se agrega además la función de garantizar la inalterabilidad del documento.

Concepto de documentos electrónicos

El avance de la tecnología con los distintos medios informáticos que brinda, se está implementando velozmente, constituyendo un fenómeno que parece presentar un



carácter irreversible, a tal punto que no es aventurado pensar que en un futuro no muy lejano, casi toda la actividad documental se llevará a cabo en forma automatizada. De ésta manera, el documento redactado en las formas tradicionales (documento manual, mecánicas o fotográficas) será prácticamente sustituido por el documento electrónico.

Al referirnos al documento electrónico se alude a que el lenguaje magnético constituye la acreditación, materialización o documentación de una voluntad ya expresada en las formas tradicionales, y en que la actividad de una computadora o de una red, sólo comprueban o consignan electrónica, digital o magnéticamente un hecho, una relación jurídica o una regulación de intereses preexistentes. Se caracterizan porque sólo pueden ser leídos o conocidos por el hombre gracias a la intervención de sistemas o dispositivos traductores que hacen comprensibles las señales digitales³². El ejemplo más común lo constituyen los documentos especialmente contruidos para el uso de los terminales de un sistema, como es el caso de las tarjetas magnéticas para acceder a las cuentas bancarias, vía cajeros automáticos.

Técnicamente el documento electrónico es un conjunto de impulsos eléctricos que recaen en un soporte de computadora, y que sometidos a un adecuado proceso, permiten su traducción a lenguaje natural a través de una pantalla o de una impresora.

Los documentos electrónicos poseen los mismos elementos que un documento escrito en soporte papel³³:

- a) constan en un soporte material (cintas, diskettes, circuitos, chips de memoria, redes);
- b) contiene un mensaje, el que esta escrito usando el lenguaje convencional de los dígitos binarios o bits, entidades magnéticas que los sentidos humanos no pueden percibir directamente;
- c) están escritos en un idioma o código determinado;
- d) pueden ser atribuidos a una persona determinada en calidad de autor mediante una firma digital, clave o llave electrónica.

³² Rolero, Graciela Lilián. Documento electrónico y firma digital. Necesidad de una legislación específica. Citado en referencia 24.

³³ Leiva, Juan. Documento Electrónico. Septiembre 2001. Obtenido de la página web www.monografias.com.

1. The first part of the paper discusses the importance of the study of the history of the United States. It is argued that the study of the history of the United States is essential for a full understanding of the country and its people. The paper then goes on to discuss the various factors that have shaped the history of the United States, including the role of the government, the economy, and the culture.

2. The second part of the paper discusses the role of the government in the history of the United States. It is argued that the government has played a central role in the development of the country, and that its actions have shaped the course of history. The paper then goes on to discuss the various ways in which the government has influenced the country, including through its policies, its actions, and its institutions.

3. The third part of the paper discusses the role of the economy in the history of the United States. It is argued that the economy has played a central role in the development of the country, and that its growth has shaped the course of history. The paper then goes on to discuss the various ways in which the economy has influenced the country, including through its production, its distribution, and its consumption.

4. The fourth part of the paper discusses the role of the culture in the history of the United States. It is argued that the culture has played a central role in the development of the country, and that its values and beliefs have shaped the course of history. The paper then goes on to discuss the various ways in which the culture has influenced the country, including through its art, its literature, and its customs.

Clasificación del documento electrónico

Lo expuesto corresponde para los documentos electrónicos en sentido estricto, los cuales se encuentran contenidos o escritos en soportes de naturaleza magnética o interna o transmitidos vía redes telemáticas³⁴. Pero existe una segunda especie de documento electrónico que surge cuando ellos son impresos computacionalmente o provienen de un sistema informatizado, es decir que ha sido plasmado al papel o llevado a la pantalla de la computadora con información proveniente de un documento electrónico en sentido estricto.

Bajo documento electrónico se comprenden datos o bien informaciones que tienen relevancia jurídica, los cuales son transmitidos o registrados por vía electrónica, especialmente a través del procesamiento electrónico de datos, pero también por medio de simples soportes de sonido.

El documento electrónico es el que está en la memoria de la máquina y cuyo contenido o texto está en el lenguaje de la máquina, el que puede ser pasado a lenguaje natural y eventualmente ser impreso para facilitar su utilización y lectura por parte de los usuarios.

Siguiendo a Giannantonio, podemos distinguir a los documentos electrónicos en³⁵:

a) Documento formado por la computadora: en éste caso la computadora no se limita a materializar una voluntad, una decisión, una regulación de intereses ya formada, sino que conforme a una serie de parámetros y datos, y a un adecuado programa, decide en el caso concreto el contenido de una regulación de intereses. La computadora no se limitará a documentar una voluntad externa, sino que determinará el contenido de tal voluntad; el lenguaje electrónico no constituye simple documentación de una voluntad en las formas tradicionales, sino que constituye la forma entendida como elemento expresivo necesario de tal voluntad, la manifestación exterior necesaria de la regulación de intereses.

³⁴ "Telemática: métodos, técnicas y herramientas de la informática aplicada". Definición extraída de la página www.angelfire.com.ar

³⁵ Giannantonio, Ettore; "El valor jurídico del documento electrónico" en "Informática y Derecho (Aportes de doctrina internacional); Ed. Depalma, año 1987.

b) Documento formado por medio de la computadora: Este es un caso distinto, pues la computadora documenta una regulación de intereses ya expresados en otras instancias o en otras formas. Aquí su actividad se dirige sólo a comprobar y no a constituir.

Son éstos últimos los llamados documentos electrónicos en sentido estricto, ya que se encuentra contenido en la memoria central de la computadora o en las memoria de masa (es decir en soportes distintos a él y, generalmente, externos: cintas, floppy disk³⁶, hard disk³⁷, CD-ROM, etc.) y cuya característica común es que no pueden ser leídos por el hombre sino a través de la actuación de una máquina que haga perceptible y comprensible la señal digital de que están constituidos.

También los documentos electrónicos pueden ser distinguidos con relación al grado de conservabilidad:

De carácter volátil, como por ejemplo los datos contenidos en las memorias ciurcuitales RAM (Random Acces Memory), los cuales se pierden inmediatamente al cortar la energía a la computadora.

Permanentes: Son aquellos contenidos en algunas memorias de masa como cintas y floppy disk. A diferencia de la anterior categoría, estos datos allí almacenados, desaparecen sólo al ser borrados, en caso contrario se mantienen en el tiempo.

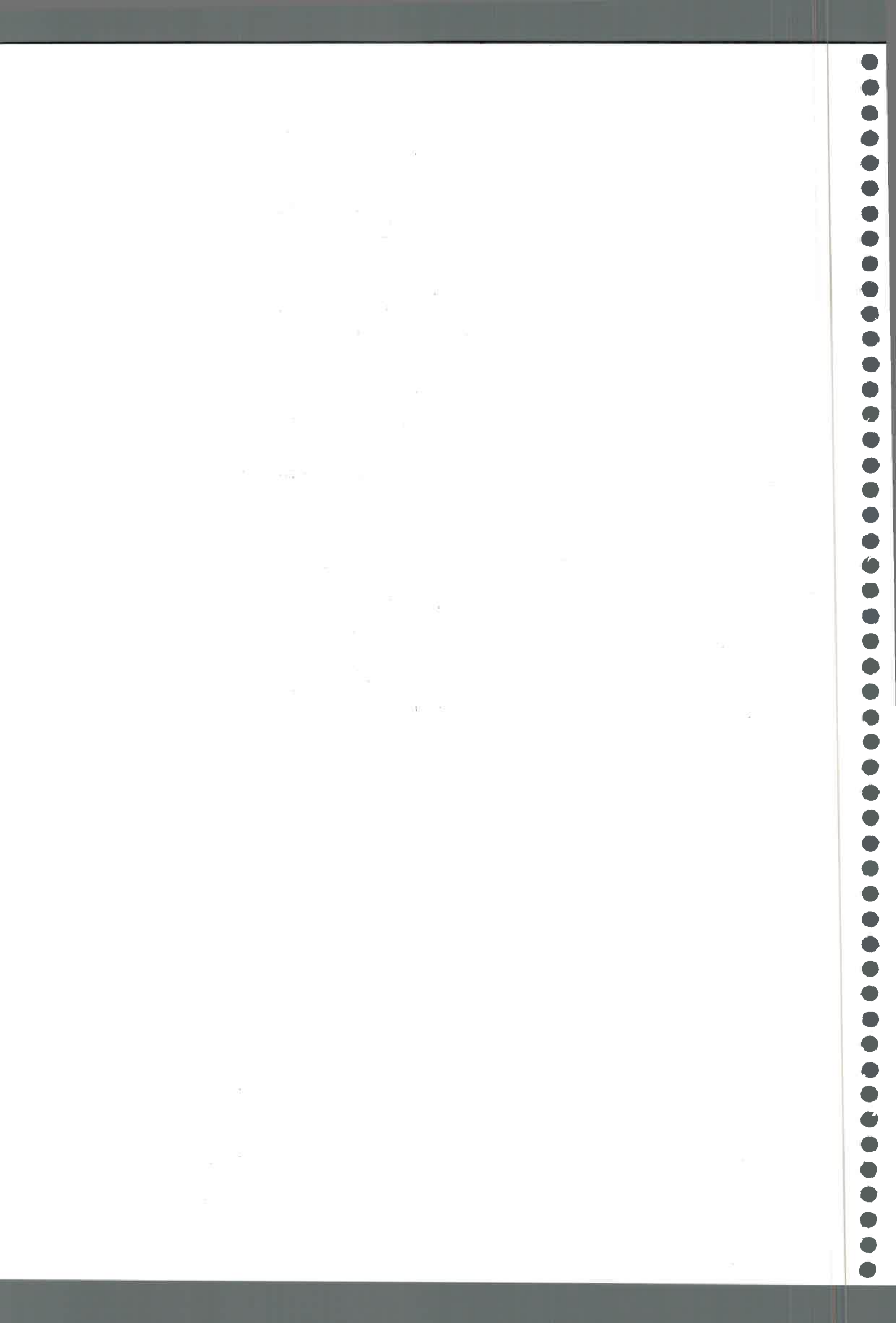
Inalterables: Son aquellos que una vez grabados no pueden ser alterados, sólo leídos. Dentro de éstos encontramos las memorias RAM (Read Only Memory), que consisten en un circuito o chip integrado a la computadora o que se le puede incorporar a la voluntad y los CD-Rom que son una memoria de masa contenida en un disco láser.

Una categoría particular de documentos en sentido estricto está constituida por aquellos documentos expresamente constituidos para el uso de las terminales de una sistema, como por ejemplo las tarjetas magnéticas para acceder a un sistema de ventas o a una cuenta corriente bancaria.

Mas allá de los documentos electrónicos en sentido estricto, existen además una serie de documentos que pueden ser formados por la computadora a través de sus órganos de salida. En tales casos no están escritos en forma digital, sino en forma de un texto alfanumérico, un diseño o gráfico estampado en soporte papel, en una tarjeta o una

³⁶ "Floppy disk: pequeños discos en los cuales es posible guardar cierta cantidad de información. También llamados discos flexibles o discos 3 1/2". Definición extraída de la página www.angelfire.com.ar.

³⁷ "Hard disk: principal fuente de almacenamiento de una computadora. También llamado disco duro". Definición extraída de la página www.angelfire.com.ar



cinta perforada, y en general, por cualquier objeto material con las características de un documento formado por una máquina conectada con una computadora.

La característica esencial de ésta categoría es que son percibibles y en el caso de los textos alfanuméricos, legibles directamente por el hombre sin necesidad de la intervención de máquinas traductoras. Podríamos decir que son copias del documento electrónico en sentido estricto.

Asimismo podemos clasificar al documento electrónico según su modo de formación:

Por intervención humana: el documento es introducido en la memoria de la computadora directamente por el hombre (por ejemplo, tecleándolo).

Por intervención de una maquina: Cuando se utiliza un lector óptico o scanner que "fotocopia" un documento escrito en papel y lo guarde en una memoria de masa.

Esta distinción tiene su relevancia jurídica en que la memorización de un documento papel preexistente puede verificarse, bien mediante la transcripción del documento en un lenguaje electrónico, bien por la reproducción en facsímil de la forma y del contenido del documento original.

En el primer caso se forma un nuevo documento, aún si su contenido es igual al del documento transcripto; en el segundo caso el documento constituye, no ya la transcripción, sino la reproducción automática de la forma y del contenido del documento original, o bien de un hecho o de un suceso. En éste último caso el órgano de inmisión no se limita a registrar sobre un soporte los caracteres alfabéticos o numéricos contenidos en el documento, sino que desarrolla una función más compleja en cuanto procede:

- A reproducir la imagen del documento;

- A dividir la imagen obtenida en una serie de elementos uniformemente distribuidos denominados PEL (Pictures Elements); y

- A transformar tales puntos en forma digital, es decir, en bits, de modo tal que pueden ser conservados en la memoria del elaborador, y eventualmente ser transmitidos a los terminales conectados.

El resultado es un documento electrónico que constituye, no la simple transcripción sino la reproducción completa y fiel de la forma y del contenido del documento original preexistente.

Documento electrónico original, duplicado y falsificado

El documento electrónico puede ser firmado o no, y en ambos casos puede haber un original y un duplicado; este último puede ser legítimamente emitido por el autor o por un tercero, o bien ser una falsificación ilegítima.

La dificultad que ofrece el documento electrónico reside en que el original es igual al duplicado, ya que los bits son idénticos.

El concepto de documento original puede ser definido por las partes o por el legislador; en este último caso, la tendencia se orienta a tomar en cuenta la primera generación, en el sentido de primera elaboración. En el proyecto de Del Piero-Molinari, en el artículo 11³⁸, se dice que “los documentos redactados en primera generación en formato digital firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, son considerados originales y poseen, como consecuencia de ello, valor probatorio como tales”.

El concepto de original y duplicado no tiene base empírica, sino que surge de una definición de las partes o del legislador que puede utilizar el criterio de la primera generación para designar el original y la segunda para referirse al duplicado.

Campo de aplicación

El documento electrónico no ofrece las seguridades que tiene el escrito, y por ello sus efectos son limitados. En general, las legislaciones son coincidentes en excluir de su campo de aplicación a:

- a) Los actos que requieren una forma especial.
- b) Los actos personalísimos, o aquellos para los cuales la ley requiera la concurrencia personal de algunas de las partes.
- c) Los actos jurídicos relativos a derecho de familia.

³⁸ Proyecto Argentino sobre Comercio Electrónico.

Estas limitaciones podrán ser superadas en el momento en que la tecnología permita que el soporte electrónico ofrezca las mismas seguridades que el escrito o que la comparecencia personal del autor.

Conservación

Uno de los problemas relevantes es el de la conservación, ya que existe la impresión generalizada de que el documento electrónico puede desaparecer en un instante y ofrece menos seguridades que el escrito. Paradójicamente, el documento electrónico se ha ido transformando en la principal fuente de archivo de la cultura escrita, ya que por razones de espacio, los documentos escritos se van traduciendo en bits para su conservación.

En una relación jurídica, las partes tienen la opción de utilizar la tecnología digital para guardar los documentos que emiten, o para hacerlos desaparecer rápidamente, ya sea que esto sea decidido por una de ellas para perjudicar a la otra, o por ambas para eludir a terceros. El problema no reside en la tecnología, sino en las obligaciones de conservación que las partes deben asumir.

El proyecto Del Piero-Molinari en el artículo 12 establece que “si la ley requiere que ciertos documentos, registros o informaciones sean conservados, tal requisito queda satisfecho mediante la conservación de los correspondientes documentos digitales, siempre que se cumplan las siguientes condiciones: que sean accesibles para su posterior consulta; que sean conservados con su formato original de generación, envío o recepción u otro formato que reproduzca en forma demostrable la exactitud del contenido del documento digital; que sea conservado, en su caso, todo dato que permita determinar el origen, destino, fecha y hora del envío y recepción.

Valor probatorio de los documentos electrónicos

Conforme aumenta el uso de Internet para celebrar contratos, van surgiendo controversias y conflictos, mismos que en muchas ocasiones requieren de una intervención judicial para llegar a un acuerdo entre las partes.

Generalmente se trata de los mismos problemas que se presentan en el comercio tradicional, pero ahora aplicados a situaciones relacionadas con el ciberespacio, donde la comunicación se realiza por medio de mensajes electrónicos.

Este es probablemente uno de los temas que pudieran tener la mayor trascendencia en las transacciones electrónicas. Hoy en día muchos dudan sobre la validez de utilizar documentos electrónicos como medio de prueba y, lo que es más grave, en ocasiones son los mismos jueces quienes se cuestionan la validez probatoria de los acuerdos y demás documentos que no constan en papel; o documentos digitales.

Probablemente la mayoría de las legislaciones establecen restricciones estrictas o taxativas a los medios de prueba, y, considerando el carácter novedoso y reciente de las tecnologías de la informática y el Comercio Electrónico, obviamente no contemplan entre sus medios de prueba a los documentos electrónicos.

El problema se acrecienta al recordar el retraso tecnológico en el Poder Judicial de muchos países. Así, se dificulta enormemente la utilización de los documentos electrónicos como medio de prueba, debido a que los funcionarios no tienen, en la mayoría de las ocasiones, la más mínima preparación técnica para operar computadoras y, consiguientemente, trabajar con este tipo de documentos.

De aquí que una de las prioridades en la reglamentación del comercio electrónico es, precisamente, reconocer el valor probatorio de este tipo de documentos, de manera de garantizar la posibilidad de exigir el cumplimiento, por lo menos en el caso de los acuerdos electrónicos, por la vía judicial.

Debemos considerar que en la valorización de las pruebas que realizan los jueces, ellos recurren necesariamente a apreciaciones y opiniones que, hasta cierto punto, pudieran calificarse como subjetivas, siempre y cuando lo hagan basándose en la razón y su experiencia. Así, entrarán a analizar ciertos elementos de la prueba, como su integridad, inalterabilidad, veracidad y exactitud.

Y, como se ha observado, gracias a los avances tecnológicos es innegable que los documentos electrónicos pueden llegar a cumplir de hecho con los requisitos de las

pruebas que analizarán los jueces, e incluso, las superan en integridad e inalterabilidad. Es por eso que en esa valoración “subjetiva” el juez deberá considerar estas características de los documentos electrónicos.

El impacto que está teniendo el comercio electrónico en el funcionamiento de la sociedad hace indispensable el adecuado reconocimiento legal de los acuerdos y demás contratos celebrados electrónicamente, de manera que sea posible utilizar los documentos digitales, o aquellos que no constan en el “papel tradicional”, como medio probatorio, perfectamente válido, en cualquier procedimiento judicial.

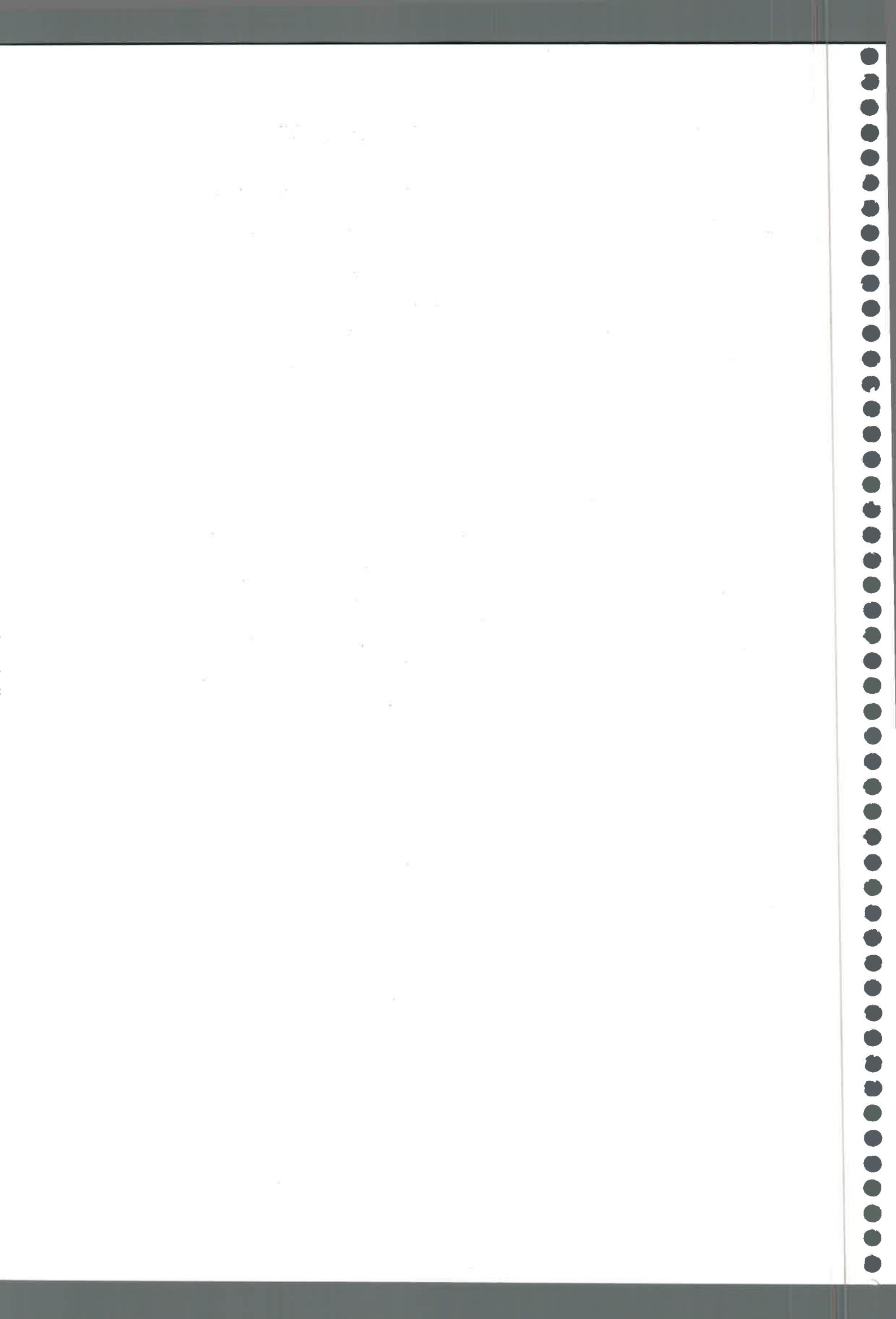
El Proyecto argentino sobre Comercio Electrónico dice: artículo 8: “Fuerza probatoria. Todos los actos jurídicos celebrados por medio de documentos digitales firmados digitalmente conforme los requisitos que esta ley dispone tendrán plena fuerza probatoria. Artículo 9: Valoración. A efectos de valorar la fuerza probatoria de los actos jurídicos celebrados por medios digitales carentes de firma digital, deberá tenerse presente la fiabilidad de la forma en que se haya generado, archivado y comunicado, conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor relevante”.

Documento electrónico como cosa

El hecho tecnológico que se manifiesta con el avance de la informática y los medios informáticos en constante evolución, vienen a modificar las relaciones entre los sujetos debido a la irrupción de nuevas modalidades y distintos procedimientos, más veloces y precisos que nos han conducido a no identificar necesariamente los títulos circulatorios o el contrato con el papel que lo contiene en vías de reemplazo por el documento electrónico. La pregunta que cabe formularse es si el documento electrónico puede ser considerado una cosa.

Digiorgio³⁹ advierte que se podría sostener que el documento electrónico constituye un objeto material de tener un valor, quedando encuadrado en la definición

39 Extraído de la página www.derechogratis.com. Consultas e información sobre legislación y jurisprudencia.



del artículo 2311 del Código Civil y además que, en algunos casos y bajo ciertas circunstancias, se puede obtener uno nuevo con iguales características, por lo que parecería sencillo entonces –dice este autor- afirmar que la mera traslación del soporte papel al soporte electrónico o magnético no desnaturaliza su calidad de documento como cosa, atento a que nuestro Código Civil únicamente hace mención al papel en su artículo 1019.

El documento debe examinarse a partir de determinados sustratos como el soporte, la forma y la prueba. En cuanto al soporte, razones de practicidad (o lo que se denomina una cultura de papel) nos han llevado a utilizar el papel como elemento preponderante pero no exclusivo.

Según opina Digiorgio, el documento electrónico puede incluirse en una categoría que había de denominarse bienes dinámicos, o más propiamente cosas dinámicas, por estar relacionadas o pertenecer a una fuerza que produce movimiento (alguno de estos objetos materiales constituyen cosas inasibles, toda vez que no pueden ser tocadas o sostenidas por las manos, criterio este que proviene de la concepción romanista). Con lo cual este autor se inclina a considerar como cosa al documento electrónico, si bien advierte que en algunas circunstancias constituyen objetos materiales intangibles, los que no se pueden percibir concretamente, esto es, no pueden percibirse de modo directo, pero que mediante la utilización de determinados procedimientos que funcionan con sus pertinentes equipos y aparatos, se pueden determinar, medir, valorar y utilizar, porque estos objetos tienen manifestaciones que llegan a nuestros sentidos y a nuestra inteligencia, ya que podemos entenderlos, ordenarlos o bien dirigirlos racionalmente, por el cual quedan encuadrados en el concepto de cosa del artículo 2311 del Código civil.

Situación en Argentina

En la Argentina existe una amplia y consolidada tendencia hacia la recepción del documento electrónico, en los campos más diversos:

1. La contabilidad electrónica.

En materia societaria, la ley 19550 en su artículo 61 dispone que “podrá prescindirse del cumplimiento de las formalidades impuestas por el artículo 53 del Código de Comercio para llevar los libros en la medida que la autoridad de control o el Registro Público de Comercio autoricen la sustitución de los mismos por ordenadores, medios mecánicos o magnéticos u otros, salvo el de inventarios y balances. La petición deberá incluir una adecuada descripción del sistema, con dictamen técnico o antecedentes de su utilización, la que una vez autorizada, deberá transcribirse en el libro de inventarios y balances. Los pedidos de autorización se considerarán automáticamente aprobados dentro de los treinta días de efectuados, si no mediare observación previa o rechazo fundado. El libro Diario podrá ser llevado con asientos globales que no comprendan períodos mayores de un mes. El sistema de contabilización debe permitir la individualización de las operaciones, las correspondientes cuentas deudoras y acreedoras y su posterior verificación, con arreglo al artículo 43 del Código de Comercio”

2. Impuestos.

Las declaraciones en materia impositiva y previsional pueden ser efectuadas por medios informáticos en una variedad de formas que han sido autorizadas por los organismos de control (resolución SAFJP 293/1997)

3. Derecho societario electrónico.

Las acciones nominativas no endosables y escriturables pueden ser registradas en medios electrónicos (artículo 6, decreto 83/1986), y pueden prescindir de la firma del director y del síndico si existe una impresión que garantice su autenticidad (artículo 212, ley 19550).

4. Administración Pública.

La ley 24624 (artículo 30) estableció, para el ámbito de la administración pública nacional, que “los documentos redactados en primera generación en soporte

electrónico u óptico indeleble a partir de originales de primera generación en cualquier otro soporte, serán considerados originales y poseerán, como consecuencia de ello, pleno valor probatorio, en los términos del artículo 995 y concordantes del Código civil”

El documento electrónico en otros países

México:

El documento electrónico o informático, se concibe como un medio de expresión de la voluntad con efectos de creación, modificación o extinción de derechos y obligaciones por medio de la electrónica, informática y telemática.

Si analizamos la noción tradicional de documento referida al instrumento en el que queda plasmado un hecho que se exterioriza mediante signos materiales y permanentes del lenguaje, vemos como el documento electrónico cumple con los requisitos del documento en soporte de papel en el sentido de que contiene un mensaje (texto alfanumérico o diseño gráfico) en lenguaje convencional (el de los bits) sobre soporte (cinta o disco), destinado a durar en el tiempo. (Legislación mexicana)

España:

“Los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos mismos medios gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos exigidos por ésta u otras leyes.”

El documento electrónico es admisible en los países de sistema de libre apreciación de la prueba, conforme a las reglas de la sana crítica para aquellos medios de prueba no excluidos en forma expresa en la ley, en este sentido, el juzgador le deberá

atribuir los efectos y fuerza probatoria después de una adecuada valoración y comprobación de autenticidad. (Legislación española)

Para Davara Rodriguez, el contrato electrónico es aquél que se realiza mediante la utilización de algún elemento electrónico cuando éste tiene o puede tener una incidencia real y directa sobre la formación de la voluntad o el desarrollo de la interpretación futura del acuerdo. En este sentido, el comercio electrónico no es sino una nueva modalidad para la formación del consentimiento, requisito esencial para la validez de los contratos. ("Davara Rodriguez, Miguel Angel. Manual de Derecho Informático Aranzadi, Madrid 1997.")

Francia:

"Los documentos emitidos, cualquiera sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos mismos medios, gozarán de validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación (...)"

Merece destacarse la legislación francesa, pues Francia es uno de los países pioneros en este campo. La ley 80/525 del 12 de julio de 1980 introdujo un trascendente cambio en el artículo 1348 de su Código Civil. En efecto, desde ese momento se estableció que el documento electrónico tendría el mismo valor probatorio que el documento en soporte papel escrito y firmado, cuando cumpliera determinados requisitos que son: inalterabilidad y durabilidad.

También los Tribunales franceses han subrayado ese mismo valor probatorio de los documentos que revisten las características marcadas por la norma.

Al margen de las citadas, los parlamentos de varios países europeos han legislado sobre el valor como prueba de los documentos electrónicos. Son legislaciones que, con algunas fallas, se muestran avanzadas en cuanto al reconocimiento de la realidad que es palpable hoy y que lo era menos hace pocos años. Al respecto la presidenta de la organización Xplor International, la Sra. Chantal Juvet, expresó en la presentación de la primera conferencia francesa de dicha asociación que el concepto de "oficina sin papel" se creó hace más de veinte años, pero como una teoría del futuro: ahora le ha llegado el turno a esa teoría.

O.N.U.:

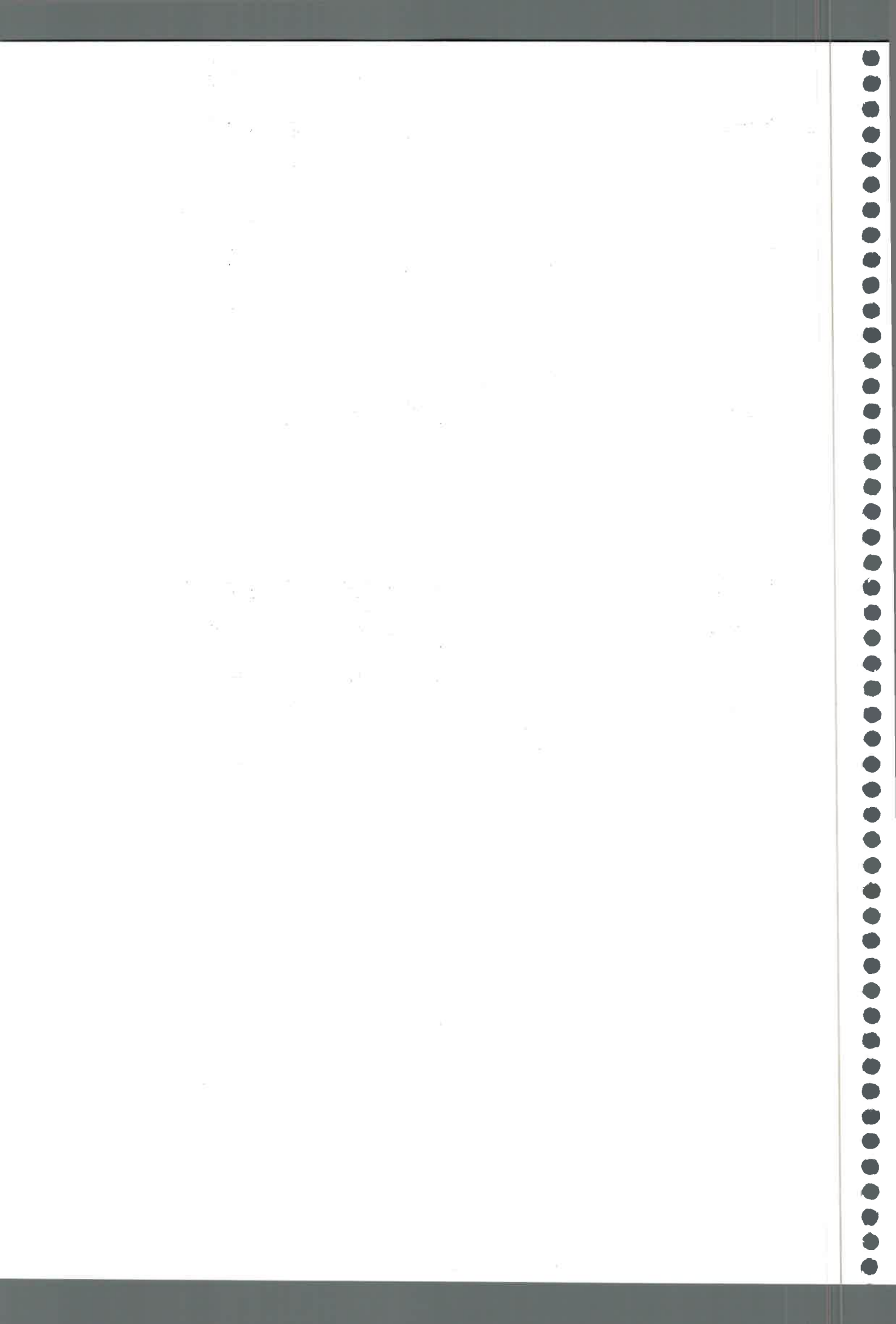
Es de destacar la actitud adoptada por las Naciones Unidas (a través de la UNCITRAL) quien, reconociendo las dificultades a que se llegue mediante la negociación a un acuerdo internacional sobre la materia, se ha decantado a favor de una rápida adecuación de las legislaciones de cada país como medida de carácter más pragmático. Es de señalar que este organismo ha emitido un valioso documento, titulado Legal Value of Computer Records, en el que se expresa que las normas o reglas concernientes a las pruebas relativas a documentos electrónicos (si bien dice registros de computadora) no deben suponer un obstáculo para el uso de las tecnologías emergentes tanto a nivel doméstico como internacional. Y señala que las normas redactadas por algunos países deben superar los problemas que genera el lenguaje empleado, pues incorpora referencias culturales que todavía suponen un freno al desarrollo.

Pero el esfuerzo de los diferentes países no es suficiente ni tiene la velocidad con la que se está desarrollando este fenómeno en la práctica. Este término, velocidad, ha adquirido una importancia fundamental por cuanto implica, en temas de tecnología la adaptación al medio con ventaja sobre el resto.

Es decir, el que llega antes en la implementación de los recursos que brindan las nuevas técnicas genera, a escala mundial, una atracción de recursos, inversiones, capitales y sobretodo de actividad. Ya dijimos antes que es un proceso imparable y más rápido que los que hayamos podido experimentar, y que conlleva un potencial incorporado en cuando a la activación de la economía y la generación de trabajo. Pero esas consecuencias beneficiosas sólo se producen en tanto los desarrollos se produzcan, al menos, al mismo tiempo que en otras partes del mundo. (Documento de la O.N.U. Legal Value of Computer Records)

Chile:

La ley 19799 publicada 12/04/2002 sobre Documento Electrónico y Firma Digital regula los documentos electrónicos y sus efectos legales, la utilización en ellos de la firma electrónica, la prestación de servicios de certificación de estas firmas y el procedimiento de acreditación al que podrán sujetarse los prestadores de dicho servicio de certificación, con el objeto de garantizar la seguridad en su uso.



La misma define en el artículo 2 inciso "d" a los documentos electrónicos como toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.

El artículo 5 establece que los mismos podrán presentarse en juicio y, en el evento de que se hagan valer como medio de prueba, habrán de seguirse las siguientes reglas: 1.-Los señalados en el artículo anterior, harán plena prueba de acuerdo con las reglas generales, y 2.-Los que posean la calidad de instrumento privado tendrán el mismo valor probatorio señalado en el número anterior, en cuanto hayan sido suscritos mediante firma electrónica avanzada. En caso contrario, tendrán el valor probatorio que corresponda, de acuerdo a las reglas generales.

República Dominicana:

Mediante el decreto 335-03, del 8 de abril de 2003, el Poder Ejecutivo dictó el "Reglamento de Aplicación de la ley No. 126-02, sobre comercio electrónico, documentos y firmas digitales". Respecto al documento digital, la ley lo define como "la información codificada en forma digital sobre un soporte lógico o físico, en la cual se usen métodos electrónicos, fotolitográficos, ópticos o similares que se constituyen en representación de actos, hechos o datos jurídicamente relevantes" (Art. 2, inciso b). El artículo 4 establece que "no se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de documento digital o mensaje de datos."

Asimismo la fuerza probatoria del documento digital reside en la confiabilidad del medio técnico que permita certeza sobre su creación, transmisión y archivo (artículo 10).

CAPÍTULO IV

La firma y la nueva tecnología

La firma es un medio para vincular un documento con su autor.

En la cultura escrita, se utilizó la grafía del autor, realizada manualmente, con toda una serie de garantías de autenticidad para ese acto, según la importancia de este. Una persona escribe debajo de un documento su nombre y apellido y se entiende que con ello declara su aceptación de aquél, su intención de obligarse.

En el mundo digital se avanza en ese sentido: se permite que el medio para vincular un documento a su autor sea una clave y no la firma holográfica.

En las relaciones jurídicas por medios electrónicos surge una cuestión de reconocibilidad: en qué condiciones existe un documento y cuándo es atribuible a su autor.

La primera respuesta a este problema es establecer una analogía directa con lo que ya conocemos, es decir, aplicar los conceptos, técnicas y reglas de la cultura escrita a la electrónica. En ese proceso encontramos el problema de que en el mundo de los átomos y la escritura, es posible realizar una comparación entre el documento original y el falso para deducir la autenticidad; es factible la prueba empírica respecto de la firma consignada en el documento; se puede tomar un papel, analizarlo, someterlo a dictámenes, hacer pericias caligráficas sobre una nueva escritura comparativa del firmante.

En el mundo virtual no es posible la prueba empírica comparativa.

El documento original puede ser igual al falso, porque no hay bits falsos; un bits hará una copia exacta de otro bits original.

En cuanto a la firma, no hay una obra de la mano del autor, no hay una firma en el sentido que se le da a la palabra en la cultura escrita. En la firma electrónica, existe la intención de reconocer la autoría, pero no necesariamente mediante el nombre y el apellido, y sin la escritura de mano propia. Por lo tanto, la noción de firma es una analogía que se utiliza para hacer más comprensible una idea.

Noción de firma

La denominada “firma electrónica” es un tema esencial para la atribución de la autoría de los documentos. Hay que destacar que si bien se habla de “firma”, ésta no está constituida por trazos manuales del autor, sino por claves, que le pertenecen de un modo indudable. El fundamento técnico para que ello sea posible lo da la criptografía, que estudia la ocultación, disimulación o cifrado de la información y los sistemas que lo permiten. A diferencia del significado que tiene en la cultura de la escritura, en este concepto de firma no tienen cabida la manualidad ni los átomos, sino las claves y los bits.

El procedimiento consiste en la transformación de un mensaje, utilizando un sistema de cifrado asimétrico, de manera que la persona que posea el mensaje inicial y la clave pública del firmante puede determinar de forma fiable si dicha transformación se hizo utilizando la clave privada correspondiente a la clave pública del firmante, y si el mensaje ha sido alterado desde el momento en que se hizo la transformación⁴⁰. La criptografía asimétrica utiliza una doble clave, pública y privada: el que envía un mensaje lo encripta con la clave pública y solo puede ser decodificado con la clave privada. La clave pública es respaldada por una autoridad certificante de su autoría; la clave privada es sólo atribuible al poseedor, y por lo tanto es asimilable a una firma en el sentido de que es un método fiable para atribuir la autoría de un documento.

La técnica criptográfica

La criptografía es un sistema que parece todavía un poco rústico, en el sentido que carece de la celeridad que sería necesaria. Sin embargo, actualmente se la admite como la técnica más difundida y segura para la firma digital, al punto que se ha convertido en estándar internacionalmente aceptado, incorporado en las normas ISO 9796; ANSI X9.31; ITU-T X.509.

⁴⁰ Definición adoptada por Ley del Estado de Utah, Estados Unidos.

La utilidad de la criptografía consiste en que provee un conjunto de símbolos cuyo significado es conocido por pocos, con lo que permite que se creen textos que serán incomprensibles a los que no conozcan los parámetros de interpretación previamente fijados⁴¹. Si las claves no pueden ser descubiertas por terceros, es un medio seguro. En este sentido la criptografía simétrica utiliza una misma clave para cifrar y luego descifrar el procedimiento, mientras que la asimétrica o de clave pública emplea dos claves, una pública y otra privada. La segunda es más confiable ya que su violación requiere averiguar las dos claves, lo cual sería difícil, por lo menos con las técnicas actuales.

El sistema de criptografía asimétrica funciona porque el emisor de una declaración de voluntad asentada en un medio electrónico le adiciona su firma que consiste en una serie de signos que conforman dos claves, una privada y una pública. El receptor recibe la clave privada, la cual es aplicada sobre el mensaje, y luego verifica éste con la clave pública. Si el resultado es positivo, se tiene garantía de la autenticidad e integridad del mensaje.

Supongamos que Baltasar (B) y Alicia (A) comparten una clave secreta, y que A recibe un mensaje cifrado supuestamente de B realizado con un sistema de criptografía simétrica. En principio, tras la recuperación exitosa del mensaje, A no tiene ninguna duda de que dicho mensaje proviene de B (autenticación), pero este esquema no es de firma digital porque B siempre puede repudiar el mensaje alegando que realmente lo produjo A.

Sin embargo, este problema se puede resolver fácilmente usando un cifrado de clave pública de la siguiente forma. B envía a A un mensaje cifrado con su clave secreta, A lo descifra con la clave pública de B, y guarda la versión cifrada. Así, si B pretende repudiar su firma, A tiene una prueba definitiva: nadie, salvo B, podría haber generado el mensaje cifrado.

En virtud de que la aplicación del sistema descrito sobre la totalidad del mensaje puede resultar costosa, especialmente si éste es muy extenso, se puede aplicar sobre el mensaje inicial el algoritmo con función hash⁴², con lo que se obtiene un resumen, caracterizado por su irreversibilidad, (esto es, a partir del resumen no puede obtenerse el mensaje completo inicial), y por ser único para ese mensaje, de forma que cualquier cambio en el mensaje produciría un resumen o hash diferente. El resumen o

⁴¹ Diniz, Davi, Monteiro. Documentos Electrónicos, Asignaturas Digitales. Ed. L Tr. San Pablo 1999

⁴² Ver definición en "Lenguaje Técnico". Página 66.

hash, de menor extensión es cifrado con la clave privada de criptografía asimétrica del firmante. Ambos mensajes, el inicial y su resumen, son enviados al destinatario, quien debe proceder a la verificación de la firma. Para ello, el verificador realizará dos operaciones: descifrará el hash firmado con la clave privada del emisor aplicando la clave pública de éste; aplicará la función hash sobre el mensaje completo que ha obtenido. Si el hash recibido y descifrado y el segundo hash obtenido coinciden, el destinatario tiene la seguridad de que el mensaje recibido ha sido firmado por el emisor con ese contenido. Si ha sido alterado en algún momento, no habrá coincidencia de los dos resúmenes⁴³.

Definiciones legales y proyectos de ley

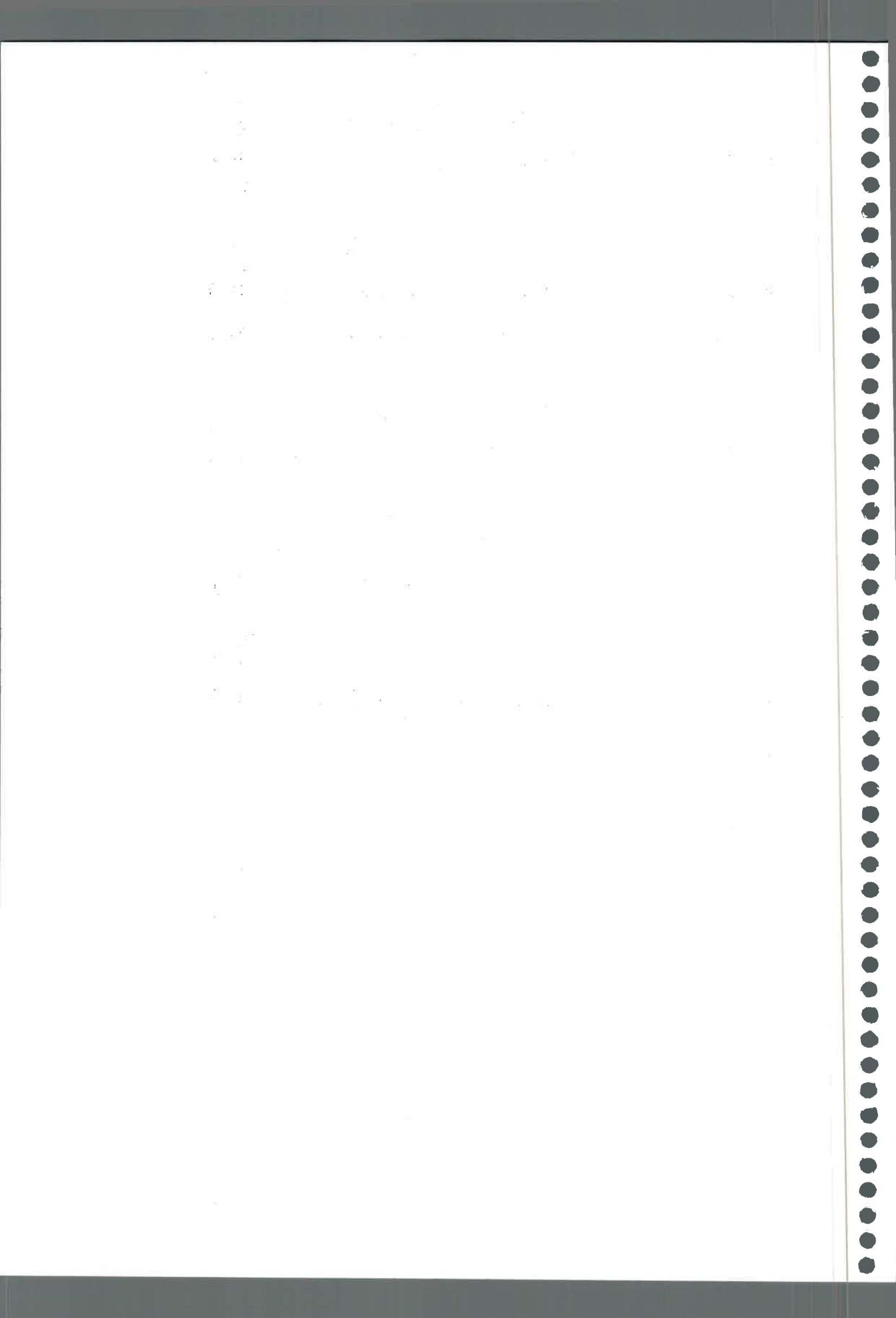
La cantidad de leyes y proyectos en el derecho comparado respecto la firma digital es numerosa, pero la desventaja que esto significa está acompañado por el beneficio de la homogeneidad, ya que casi todos ellos siguen el mismo modelo.

En la definición de Uncitral⁴⁴ se dice, en el artículo 7, que cuando la ley requiera la firma de una persona, ello se considerará cumplido cuando haya sido utilizado algún método para identificar a la persona e indicar su aprobación del contenido de un mensaje electrónico y ese método haya sido confiable.

La ley de firma digital del estado de Utah (del 27/2/1995) ha sido el modelo más seguido y citado, junto con el de Uncitral; dispone que la firma digital requiere la autenticación del remitente, la integridad del mensaje y que éste no pueda ser negado, y para ello adopta el sistema de criptografía asimétrica; incluye definiciones sobre autoridad certificante, aceptación, criptografía asincrónica, firma digital, a los fines de dar significado normativo al tecnolenguaje informático. La firma digital tiene los efectos de la escrita, si está verificada como referida a una clave pública contenida en un certificado válidamente extendido por una autoridad certificante y si esa firma digital ha sido estampada por el firmante con la intención de firmar el mensaje, el destinatario de

⁴³ Martínez Nadal. La ley de firma electrónica. Madrid 2000.

⁴⁴ Ley Modelo sobre Comercio Electrónico- Comisión de las Naciones Unidas (UNCITRAL)



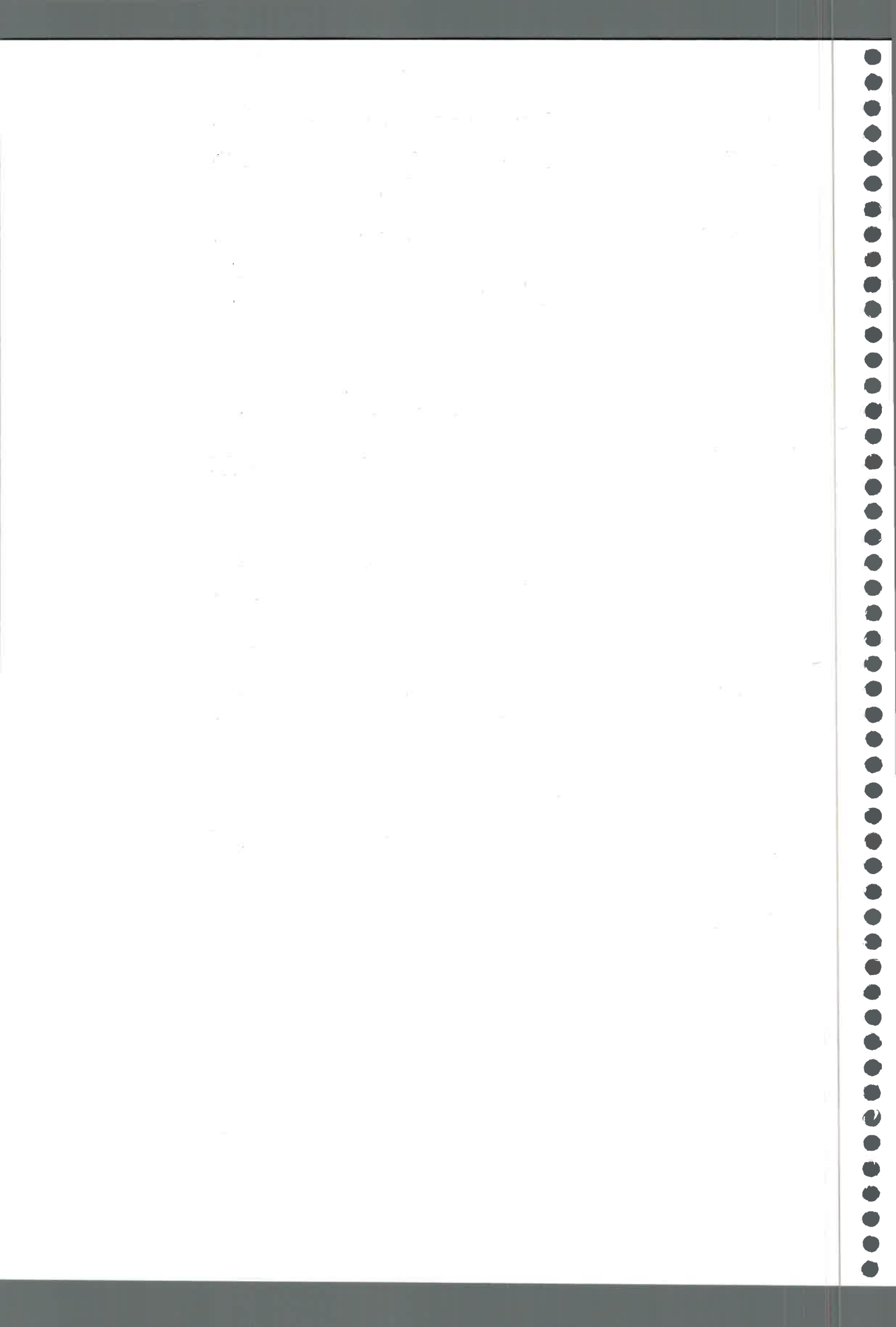
una firma digital asume el riesgo de que ésta haya sido falsificada si no existen razonables condiciones de confiabilidad. Si el destinatario decide no confiar en las disposiciones sobre firma digital, debe hacerlo saber inmediatamente al firmante.

La Electronic Signatures in Global and National Commerce (1999), define la locución "electronic signature", como la información o datos en forma electrónica, vinculados o asociados en forma lógica con un registro electrónico, y adoptados por una persona o un agente electrónico de una persona, con la intención de firmar un contrato o documento. El término "electrónico" significa toda tecnología que incluya medios eléctricos, digitales, magnéticos, ópticos, electromagnéticos o similares; la frase "agente electrónico" se refiere a un programa de computación u otro medio usado para estos fines.

La Electronic Signature Record Act (Nueva York, 1999) define en general la firma electrónica como un medio electrónico de identificación, que incluye la firma digital, la cual es única para la persona que la usa, susceptible de verificación, sujeta al único control de la persona que la utiliza, está asociada con datos que garantizan su autenticidad y su integridad y es usada por su titular para que tenga la misma fuerza que la firma a mano.

La Directiva de la Unión Europea sobre un Sistema Común para Firmas Electrónicas, del 24/5/1999, señala que la firma electrónica adjuntada a un documento electrónico tiene exactamente el mismo valor legal que la firma manuscrita adjuntada a un documento escrito en soporte de papel y admite como medio de prueba la firma electrónica asociada a un documento electrónico. Se establece un sistema voluntario de acreditación de los prestadores de servicios de certificación, y se especifica que éstos serán responsables, ante cualquier persona que de buena fe haya confiado en el certificado, de conformidad con la ley y de la veracidad de su contenido. Esta responsabilidad se encuentra objetivada, puesto que el prestador de servicios de certificación se exime de responsabilidad en cuanto demuestra haber actuado siempre con la máxima diligencia para comprobar la información proporcionada por la persona certificada, invirtiéndose de este modo la carga de la prueba.

En España, el real decreto ley 14/1999 dice que la firma electrónica "es el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente a ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge".



En Alemania, en la Ley Federal aprobada por el bundestag el 13/6/1997, se define a la firma digital como un sello creado con una clave privada de firmas sobre información digital; tal sello permite, mediante el uso de la clave pública asociada, rotulada por un certificado de clave de un certificador, que sean verificados el propietario de la clave de la firma y el carácter de no falsificado de la información.

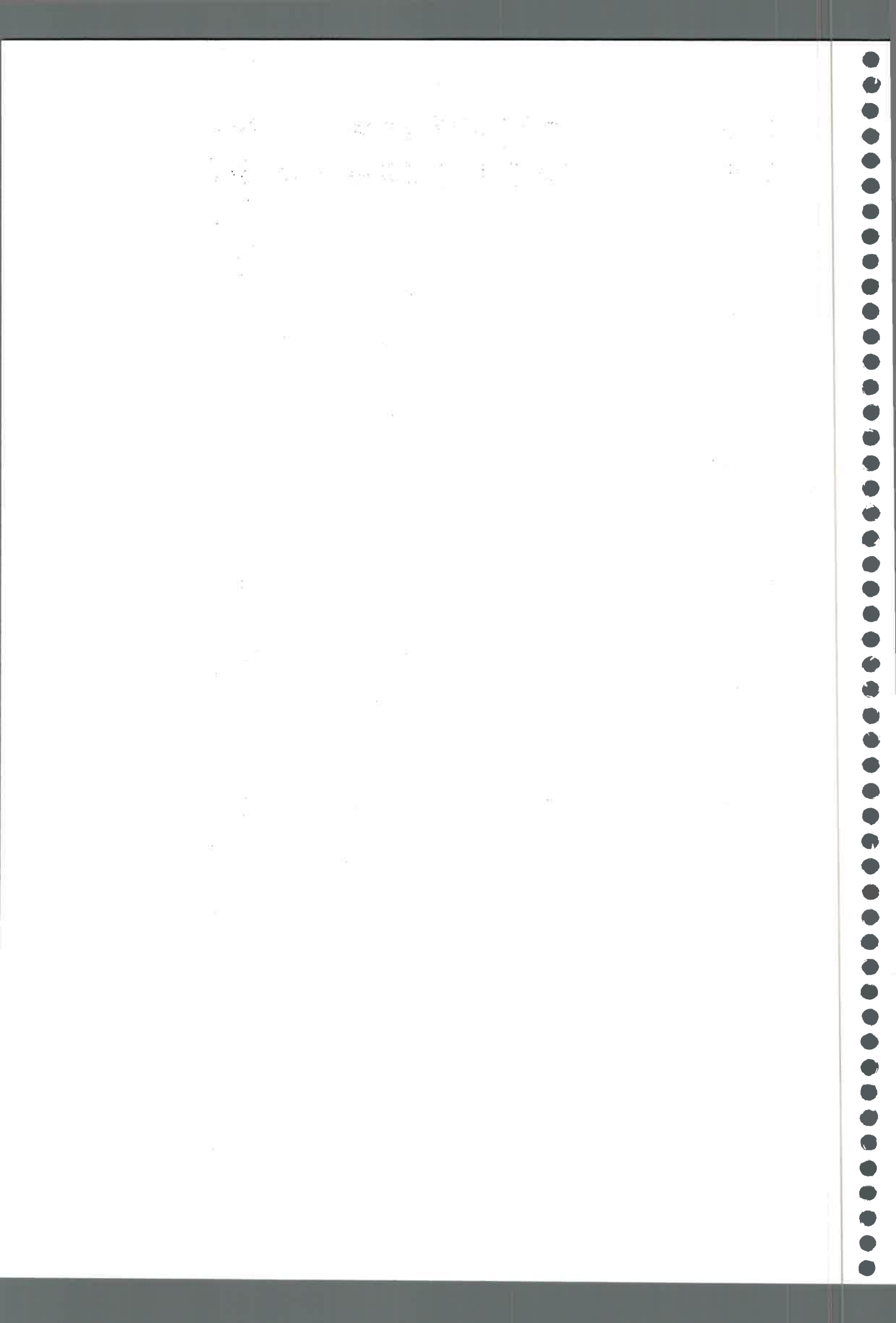
En Portugal, en el decreto ley 290/99 del 2/8/1999 y decreto ley 375/1999, la define diciendo que es el proceso de firma electrónica basado en un sistema criptográfico asimétrico compuesto de un algoritmo o serie de algoritmos, mediante el cual se generan un par de claves asimétricas exclusivas e interdependientes, una de las cuales es privada y la otra pública, y que permite al titular usar la clave privada para declarar la autoría del documento electrónico al cual la firma se refiere en concordancia con su contenido, y al destinatario usar la clave pública para verificar si la firma fue creada mediante el uso correspondiente de la clave privada o si el documento electrónico fue alterado después de puesta la firma. Se dice también que el régimen previsto se aplicará a otras modalidades de firma que satisfagan exigencias de seguridad idénticas a la firma digital.

La ley colombiana 527/1999 dice que la firma digital es un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje, permite determinar que este valor ha sido obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación.

En Perú, la ley 27269 en el artículo 1, dice que la misma tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad. Se entiende por firma electrónica cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita. En el artículo 2 se dice que se aplica a aquellas firmas electrónicas que, puestas sobre un mensaje de datos o añadidas o asociadas lógicamente a ellos, puedan vincular o identificar al firmante. Así como garantizar la autenticación e integridad de los documentos electrónicos.

En cuanto a los proyectos de ley podemos señalar las siguientes:

Proyecto de ley de Firma Digital de la República Argentina del año 1999, que se desarrollará más adelante.



En el proyecto argentino Del Piero-Molinari sobre Comercio Electrónico se define a la firma digital en el artículo 2 como “los datos expresados en formato digital, utilizados como método de identificación de un firmante y de verificación de integridad del contenido de un documento digital, que cumpla con los siguientes requisitos: pertenecer únicamente a su titular; encontrarse bajo su absoluto y exclusivo control; ser susceptible de verificación, estar vinculada a los datos del documento digital de modo tal que cualquier modificación de los mismos ponga en evidencia su alteración.

El proyecto de reformas del Código Civil argentino de 1998 establece en el artículo 266 que “ la firma prueba la declaración de voluntad expresada en el texto al cual corresponde. Debe ser manuscrita y consistir en el nombre del firmante, o en un signo, escritos del modo en que habitualmente lo hace a tal efecto. En los instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho si se utiliza un método para identificarla; y ese método asegura razonablemente la autoría e inalterabilidad del instrumento”.

Firma electrónica y firma digital

La firma electrónica es un género, caracterizada por el soporte: todo modo de identificación de autoría basado en medios electrónicos es firma electrónica. Luego vienen las especies que en general se caracterizan por agregar elementos de seguridad que la sola firma electrónica no posee. Las legislaciones reconocen el género de firma electrónica y luego eligen una especie dentro de él, que denominan “firma electrónica avanzada”, o “firma digital”, que es la que utiliza un sistema, generalmente criptográfico, que da seguridad. La gran diferencia estriba en que cuando se utilice la firma digital, se aplican presunciones sobre la identidad del firmante y la integridad del documento que suscriba⁴⁵.

De este modo podemos nombrar algunas definiciones:

⁴⁵ Lorenzetti, Ricardo. Comercio Electrónico. Citado en referencia 1.

1. The first part of the document is a list of names and their corresponding numbers. The names are written in a cursive script, and the numbers are written in a simple, bold font. The list is organized into two columns, with the names on the left and the numbers on the right. The names are: John, James, William, Robert, Thomas, Richard, Henry, George, Edward, and Charles. The numbers are: 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10. The list is as follows:

Name	Number
John	1
James	2
William	3
Robert	4
Thomas	5
Richard	6
Henry	7
George	8
Edward	9
Charles	10

Name	Number
John	1
James	2
William	3
Robert	4
Thomas	5
Richard	6
Henry	7
George	8
Edward	9
Charles	10

3. The third part of the document is a list of names and their corresponding numbers. The names are written in a cursive script, and the numbers are written in a simple, bold font. The list is organized into two columns, with the names on the left and the numbers on the right. The names are: John, James, William, Robert, Thomas, Richard, Henry, George, Edward, and Charles. The numbers are: 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10. The list is as follows:

Name	Number
John	1
James	2
William	3
Robert	4
Thomas	5
Richard	6
Henry	7
George	8
Edward	9
Charles	10

Firma electrónica: En la ley modelo de Uncitral se utiliza un concepto general y flexible en su artículo 7, que identifica la firma con un método que tiene por función identificar al iniciador del mensaje y confirmar que el iniciador aprueba la información en él consignada. El grado de seguridad que se puede lograr debe ser tan fiable como sea apropiado a los fines para los que se generó o comunicó el mensaje de datos, a la luz de las circunstancias del caso, incluido cualquier acuerdo pertinente. En el proyecto Del Piero-Molinari se dice en el artículo 5 que la firma electrónica está constituida por “ los datos en forma electrónica asociados a otros datos electrónicos o vinculados de manera lógica con ellos, utilizados como medio de identificación, que no reúne uno o más requisitos para ser considerada como firma digital”

Firma electrónica segura: teniendo en cuenta lo anteriormente dicho, una firma segura es la que tiene algún elemento adicional para verificar su autenticidad. Mediante este procedimiento, que puede ser muy variado, según las diferentes legislaciones, acuerdo de partes y tecnologías existentes, la firma puede ser verificada como perteneciente a una específica persona en forma rápida, objetiva e indubitable, sin posibilidades de que sea repudiada por su autor.

Firma electrónica avanzada: La Directiva Europea del 13/5/1998 y varias leyes, como la ley española, recogen el concepto de firma electrónica avanzada, definido como “la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refieren, lo que permite que sea detectable cualquier modificación posterior de éstos”. El proyecto chileno dice que es aquella creada mediante medios que el titular mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, y permite que sea detectable cualquier modificación ulterior de éstos, garantizando así la identidad del titular y que éste no pueda desconocer la autoría del documento y su integridad.

Firma digital: La ley peruana establece que firma digital es aquella firma electrónica que utiliza una técnica criptográfica asimétrica, basada en el uso de un par de claves único, asociadas a una clave privada y una clave pública relacionadas matemáticamente entre si, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada. En el proyecto Del Piero-Molinari se dice que la firma digital es

el resultado de la transformación de un documento digital por medio de un sistema informático, que cumple con los siguientes requisitos:

- a) ser exclusiva del signatario;
- b) ser susceptible de verificación;
- c) estar bajo resguardo y control absoluto el signatario;
- d) que el documento digital esté encriptado con la clave privada del signatario, de manera tal que, si el mensaje sufre alguna modificación, la firma quede invalidada;
- e) que la persona que posea el documento digital inicial, el encriptado y la clave pública del signatario pueda determinar con certeza que la transformación fue realizada utilizando la clave privada correspondiente a dicha clave pública y que el documento original no ha sido modificado desde que se efectuó;
- f) que haya sido adoptado como norma por no menos de dos de las siguientes organizaciones: UIT, ANSI, ISO, UNCITRAL;
- g) que la transformación del mensaje se haya realizado empleando un criptosistema asimétrico.

Elementos que caracterizan a la firma digital

Los mismos son⁴⁶:

-Elemento objetivo-soporte: En un sentido negativo, el soporte no es escrito, y no hay una elaboración manual del autor. En un sentido positivo, la firma es cualquier símbolo o procedimiento de seguridad usado por una persona que incluye medios eléctricos, digitales, magnéticos, ópticos, electromagnéticos o similares. Puede advertirse, entonces, que la firma electrónica no necesariamente debe ir anexada a un documento, como ocurre en el caso de la firma holográfica sobre un documento escrito.

-Elemento subjetivo: Los símbolos asentados en medios electrónicos tienen un propósito específico: se hacen para identificar a la persona e identificar su aprobación del contenido de un mensaje electrónico.

⁴⁶ Lorenzetti, Ricardo. Comercio Electrónico. Citado en referencia 1.

Con estos dos elementos puede haber firma electrónica, pero para que la ley asigne efectos de presunción, es decir, que cada vez que se vean esos signos se presuma que son de su autor se requiere además:

-Esfera de control del titular: Siendo un elemento de imputación de autoría, es lógico que se requiera que esté bajo el control del titular, ya que solo él es quien decide qué declaraciones de voluntad son suyas. Por ello es necesario que la firma pertenezca únicamente a su titular y se encuentre bajo su control exclusivo.

-Derechos de verificación del receptor: Se requiere que los sistemas utilizados puedan ser verificados por el receptor para asegurarse de la autoría.

Funciones de la firma digital

-Garantizar la autoría: ésta es la función esencial de la firma, en cuanto permite relacionar un documento con su autor, imputándole a su esfera de intereses los efectos jurídicos de la declaración que obra en un soporte determinado. La firma escrita es dependiente del documento que la recibe y conserva; en cambio, la firma digital implica una secuencia de números y bits independientes del documento, ya que contiene, por sí sola, la información suficiente para que pueda ser conocido el titular y determinar si hubo alteraciones; el soporte documental no es indispensable.

-Mantener la confidencialidad del mensaje: en el soporte electrónico, la confidencialidad es un elemento imprescindible, puesto que existen riesgos importantes en relación con su captura por parte de terceros.

-Posibilitar el control de acceso limitado: como no hay firma holográfica, es necesario que las partes puedan verificar la exactitud de las claves utilizadas.

-Mantener la integridad de la información: en el medio electrónico existe el riesgo de modificación por parte de terceros, de modo que el mensaje llega, es imputado al autor, pero no es la misma declaración.

-Asegurar la validez probatoria y los plenos efectos de la firma escrita: este aspecto tiene relación con la celeridad de los negocios y la disminución de los costos de transacción; es necesario que la firma sea suficiente prueba de autoría, porque de lo contrario sería muy costoso el tráfico jurídico.

Efectos

En general, la firma digital tiene los mismos efectos que la escrita y no se le puede negar validez sobre la sola base de que no está de forma escrita. Se le adjudican los siguientes efectos:

- Presunción de autenticidad: la firma electrónica que cumple con los requisitos de certificación se presume auténtica correspondiente al autor, y revela su intención de obligarse.

-Presunción de integridad: se presume que los datos no han sido alterados desde el momento en que la firma electrónica fue añadida a ellos. En efecto: la “firma digital” sólo existe en la medida en que se envíe con un documento digital. En el mundo material es concebible la existencia de una firma manuscrita sobre un papel en blanco y que en el papel se escriba luego de firmado. Cuando se firma digitalmente, nada puede ponerse en el documento con posterioridad a ser firmado, porque la vinculación entre “documento” y “firma” lo hace un todo indisoluble. Si algo se altera, el certificado lo avisa. Si se manda un correo electrónico firmado digitalmente, éste no puede abrirse y cambiarse su contenido sin afectar su vinculación con la firma certificada. Con que sólo se intente este supuesto, el certificado avisaría que el mensaje fue violado y la firma perdería su validez.

- La carga de la prueba corresponderá a la parte que niegue su validez.

-Las partes intervinientes no podrán rechazar las obligaciones contractuales derivadas del negocio llevado a cabo, salvo en el caso de que demuestren que concurre algún vicio del consentimiento previsto en la legislación nacional, o cualquier otra prueba que desvirtúe la presunción.

-La legislación debe prever los procedimientos de impugnación de los documentos firmados bajo coacción, mala fe, fuerza o engaño.

Campo de aplicación

Como principio general, no hay ninguna norma que prohíba el uso de firmas digitales y documentos electrónicos, de modo que las partes pueden utilizar la forma que desean. La configuración de las normas no es de prohibición, si no de permisión, es decir que autorizan a determinadas formas a tener determinados efectos. Si la norma que atribuye esos efectos no lo hace en forma excluyente, como ocurre cuando hay formas *adsolemnitaten*⁴⁷, nada impide que las partes establezcan el modo de documentar y firmar.

Esto significa que las partes pueden acordar que en sus relaciones darán validez a documentos y firmas electrónicas, y ese acuerdo no puede ser rechazado judicialmente sobre la sola base de que no requiere la forma escrita. Sin embargo, para disminuir los costos de transacción y para darle al acuerdo oponibilidad frente a los terceros es necesaria la ley.

Se admite, en general que la firma digital tiene su principal campo de utilidad en las relaciones comerciales y por ello la legislación excluye su aplicación a:

- las disposiciones por causa de muerte;
- los actos jurídicos del derecho de familia;
- los actos personalísimos en general;
- 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 de acuerdo de partes.

⁴⁷ "Forma *adsolemnitatem*: requieren una forma bajo pena de nulidad, pues la forma es de la esencia estructural del acto o negocio". Santos Cifuentes. Elementos del derecho civil. Parte General. Ed. Astrea

En algunas legislaciones se prevé específicamente la aplicación de la firma digital en las relaciones de consumo. Por ejemplo, la Electronic Signatures in Global and National Commerce, dice que si la ley requiere que se entregue un documento escrito al consumidor, aquél puede ser dado bajo forma electrónica si el consumidor ha consentido afirmativamente y en forma separada este procedimiento y si previamente al consentimiento se le provee el hardware y el software necesarios para acceder y conservar el registro electrónico.

Riesgos de la firma digital

La regla es que el destinatario de una firma digital asume el riesgo de que ésta haya sido falsificada si no existen razonables condiciones de confiabilidad. Si el destinatario decide no confiar en las disposiciones sobre firma digital, debe hacerlo saber inmediatamente.

1. Riesgos de la ineficacia.

En el proyecto Del Piero-Molinari, en el artículo 8, se establece que “una firma digital es válida si cumple con los siguientes requisitos: haber sido creado durante la vigencia de un certificado digital válido; haber sido debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado; que dicho certificado haya sido emitido por un certificador licenciado por la autoridad de aplicación.

2. Riesgos en la generación de los datos de firma.

Existe un riesgo en la generación de los datos: las claves pueden ser inseguras, poco fiables, conocidos por terceros, repetidas o de baja calidad.

Estos riesgos disminuyen a medida que se mejora la calidad de las instituciones que administran las claves que se les imponen requerimientos legales.

Para mejorar la seguridad se establecen procedimientos: claves dobles, públicas y privadas, como ocurre con la criptografía; claves irreversibles, de modo que el

enlazamiento no pueda romperse en un período de tiempo preestablecido; claves que no puedan ser traducidas, en el sentido de que sea inviable conocer la clave privada secreta a través de la clave pública; claves únicas y exclusivas, de manera que no puedan duplicarse ni ser conocidas ni estar disponibles para otro sujeto que no sea el titular.

3. Riesgo de la difusión de las claves.

Las firmas manuales tienen una asociación intrínseca con una persona determinada, porque están hechas con la escritura manual única del firmante; sin embargo, un juego de claves usado para crear una firma digital no tiene una asociación intrínseca con nadie: un bit es exactamente igual que otro bit; el par de clave pública y privada no tiene asociación intrínseca con ninguna persona; es, simplemente, un par de números. Por ello es necesaria una forma segura de asociar a una determinada persona o entidad con un par de claves.

Existen problemas con la difusión de las claves, porque si esto ocurre, la firma puede ser usada por cualquiera constituyendo un grave riesgo para el autor.

En el sistema de doble clave, es necesario que el destinatario tenga acceso a la clave pública para verificar si corresponde la clave privada. Consecuentemente, se plantea un problema con la entrega de esas claves. Una de las soluciones es la entrega manual de claves públicas, que se hace juntamente con garantías de seguridad y de secreto.

Este sistema de intercambio manual es adecuado y eficaz para pequeños grupos de personas entre las que se da una mutua cooperación y confianza.

Para grupos más amplios, se utiliza la participación de terceros de confianza, que emiten certificados que, a la vez que sirven para distribuir la clave pública, permiten esencialmente asociar de forma segura la identidad de una persona concreta a una clave pública determinada.

Certificación

La firma digital requiere un marco institucional que produzca confianza.

Puede haber una firma de este tipo mediante un acuerdo celebrado entre dos partes, las cuales se obligan a reconocerla según los criterios que los contratantes fijen. Sin embargo, el costo de negociar estos acuerdos es alto entre partes que no se conocen o que están situadas en lugares lejanos y no tienen referencias. Por ello, para que exista un uso difundido, rápido, se utiliza un tercero que certifica.

La figura del tercero otorga confianza y disminuye los costos de transacción.

El problema es quién es ese tercero, qué hace y con qué extensión.

En la práctica comercial han surgido organizaciones que proveen de certificados y que se hacen confiables por su conducta y el apoyo que van logrando en la comunidad. La expansión de estos procedimientos de adhesión voluntaria se produce, habitualmente, en grupos cerrados o que reconocen algún límite, pero es difícil para ellos lograr un reconocimiento generalizado de su actuación. Por esta razón, muchas legislaciones regulan un sistema institucional que requiere el registro de las autoridades certificadoras.

Autoridades certificadoras

Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismos públicos que expide certificados o presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por la autoridad de aplicación. Sus funciones son emitir certificados digitales de acuerdo con lo establecido en sus políticas de certificación, identificar inequívocamente los certificados digitales emitidos y mantener copia de todos ellos⁴⁸.

Se ha postulado la intervención de un escribano en estos casos y se lo ha denominado “cibernotary”, lo cual no tiene otro significado que el de admitir que un escribano cumpla funciones de autoridad certificadora de firmas digitales⁴⁹.

⁴⁸ Del Piero-Molinari. Proyecto sobre Comercio Electrónico

⁴⁹ Devoto Mauricio. Claves para el éxito de una infraestructura de firma digital. 24/2/2000

El certificado de clave públicas es otorgado por el certificador y relaciona la clave pública con su suscriptor. Cuando actúa un escribano, las autoridades certificadoras delegan la recepción de la solicitud o aplicación y la consecuente identificación del interesado en las autoridades de registro, que son los notarios de tipo latino. El cibernotario tiene la función de realizar una investigación de los usuarios que deseen registrar sus claves públicas para utilizarlas en el comercio electrónico. Puede existir una certificación de bajo valor, donde se establece la identidad del usuario para una clave pública, o una de alto valor, donde el notario realiza una investigación sobre la historia crediticia y criminal del usuario antes que la clave sea emitida.

Algunos autores se han mostrado muy críticos respecto de la posibilidad de que los notarios actúen en este campo, considerando que tratan de mantener una suerte de reserva de mercado o feudo, postulando la libre concurrencia para que cualquier entidad que reúna unos requisitos igualitarios puedan ofrecer el servicio⁵⁰.

Eficacia del certificado

El certificado digital tiene por función básica la de autorizar la comprobación de la identidad del firmante, pero además debe permitir que el titular lo reconozca indubitadamente y conozca su período de vigencia; determinar que no ha sido revocado; reconocer claramente la inclusión de información no verificada; especificar tal información; contemplar la información necesaria para la verificación de la firma; identificar claramente al emisor del certificado digital⁵¹. El artículo 2.9 de la Directiva de la Unión Europea dice que el certificado es la certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de ésta.

Los certificados tienen una eficacia limitada, que el legislador dispone. Las causas de la misma son:

- a) expiración del período de validez;
- b) revocación por el signatario;

⁵⁰ Lorenzetti, Ricardo. Comercio electrónico. Citado en referencia 1.

⁵¹ Del Piero-Molinari. Proyecto sobre Comercio Electrónico.

- c) pérdida o inutilización por daños del soporte del certificado;
- d) utilización indebida por un tercero;
- e) resolución judicial o administrativa que lo ordene;
- f) fallecimiento del signatario o de su representado, incapacidad sobrevenida, total o parcial, de cualquiera de ellos, terminación de la representación o extinción de la persona jurídica representada;
- g) cese en su actividad del prestador del servicio de certificación, salvo que, previo consentimiento expreso del signatario, los certificados expedidos por aquél sean transferidos a otro prestador de servicio;
- h) inexactitudes graves en los datos aportados por el signatario para la obtención el certificado.

La pérdida de eficacia debe ser publicitada para que sea oponible a los terceros.

Obligaciones del certificante

Conforme con el proyecto Del Piero-Molinari, en el artículo 18, se establece que son obligaciones del certificador licenciado: 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; mantener el control exclusivo de sus propios datos de creación de firma digital e impedir su divulgación; mantener la confidencialidad de toda información que no figure en el certificado digital; poner a disposición del solicitante de un certificado digital toda la información relativa a su tramitación; mantener la documentación respaldatoria de los certificados digitales emitidos por diez años a partir de su fecha de vencimiento o revocación. Los certificados son revocados por su titular, mediante un trámite que se realiza ante la autoridad de aplicación. El certificado no es válido si es utilizado para alguna finalidad contraria a aquellas para las cuales fue extendido; para operaciones que superen el valor máximo autorizado para su validez, o una vez revocado.

Derechos de los titulares y usuarios de firmas electrónicas

Los titulares y usuarios de firmas electrónicas celebran un contrato para la provisión de este servicio, que está regulado en la ley que crea el servicio o bien, en ausencia de texto legislativo expreso, puede ser calificado como un contrato de servicios profesionales.

Se trata de una relación entre un experto y un ignorante, y por lo tanto, caracterizada por acentuados deberes colaterales de cooperación y de información del proveedor hacia el tomador del servicio. Puede darse el caso de que resulte aplicable la ley de defensa del consumidor, en todos los supuestos en que hay un consumo final, como lo califican los diversos ordenamientos.

También hay que destacar que se pone bajo la custodia del proveedor una serie de datos personales de la mayor relevancia, y sobre las cuales hay una obligación de seguridad y de secreto o confidencialidad. Estos deberes colaterales surgen claramente de la prestación, y su incumplimiento obliga a indemnizar.

En el artículo 23 de la ley chilena N° 19799 sobre Firma y Documento Electrónico hay un interesante desarrollo del tema, donde se destacan los siguientes derechos del usuario:

1) A ser informado por el prestador de servicios de certificación de las características generales de los procedimientos de creación y de verificación de firmas electrónicas, así como de las reglas sobre prácticas de certificación y las demás que aquél se comprometa a seguir en la prestación del servicio, previamente a que se empiece a efectuar.

2) A que el prestador de servicios de certificación emplee alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el usuario y a que se le informe, previamente al inicio de la prestación del servicio, de las características generales de dichos elementos.

3) A ser informado, antes de la emisión de un certificado, del precio de los servicios de certificación, incluyendo cargos adicionales y formas de pago; de las condiciones precisas para la utilización del certificado y de sus limitaciones de uso; de la acreditación del prestador de servicios, si corresponde, y de los procedimientos de reclamación y de resolución de litigios previstos en las leyes o que se convinieren.

4) A que el prestador del servicio o quien homologue sus certificados le le proporcionen la información sobre sus domicilios y sobre todos los medios a los que el usuario pueda acudir para solicitar aclaraciones, dar cuenta del mal funcionamiento del sistema o presentar sus reclamos.

5) A ser informado, al menos con dos meses de anticipación, por los prestadores de servicios de certificación, del cese de su actividad, con el fin de hacer valer su oposición al traspaso de los datos de su certificado a otro certificador, o bien para que tomen conocimiento de la extinción de los efectos de sus certificados, si no existiere posibilidad de traspaso a otro certificador.

6) A ser informado inmediatamente de la cancelación de la inscripción en el registro de prestadores acreditados, con el fin de hacer valer su oposición al traspaso de los datos de su certificado a otro certificador, en cuyo caso dichos certificados se extinguirán, o bien, para tomar conocimiento de la extinción de los efectos de sus certificados, si no existiere posibilidad de traspaso a otro certificador.

7) A traspasar sus datos a otro prestador de servicios de certificación.

8) A que el prestador no proporcione más servicios y de otra calidad que los que haya pactado, y a no recibir publicidad comercial de ningún tipo por intermedio del prestador.

9) A acceder, por medios electrónicos, al registro de prestadores acreditados y al registro especial de prestadores no acreditados que mantendrá la entidad acreditadora.

10) A ser indemnizado y hacer valer los seguros comprometidos.

Responsabilidad de la autoridad certificante

En la legislación de la Unión Europea se prevé que respondan por los daños que causen a cualquier persona, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone la ley o actúen con negligencia. Es decir, se adopta un sistema de responsabilidad por culpa que será contractual frente a las partes y extracontractual frente a terceros. Los supuestos de responsabilidad más relevantes son:

a) fallas en veracidad de las afirmaciones que contiene el certificado en el momento de su expedición; b) fallas en la garantía de que obran en poder del firmante identificados los datos de creación de la firma a que hace referencia el certificado; es decir, que la

autoridad de certificación comprobó en forma deficiente que el solicitante tiene la clave privada correspondiente a la clave pública del sujeto del certificado.

Según el proyecto Del Piero-Molinari, en el artículo 28, “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”. También se afirma, en el artículo 29, que el certificador que emita un certificado digital es responsable por los incumplimientos a las previsiones de la presente ley, por los errores y omisiones que presenten los certificados digitales que expida, por no haberlos revocado en legal tiempo y forma cuando así correspondiere y por las consecuencias imputables a la inobservancia de procedimientos técnicos de certificación exigibles. En el artículo 30, se establece que “sólo pueden eximirse de tal responsabilidad cuando demuestren: que han adoptado las debidas medidas para evitar los errores u omisiones; que han procedido a la revocación del certificado digital inmediatamente de notificada la solicitud o confirmada su procedencia si fuera requerida por un tercero”.

El lenguaje técnico

Muchas legislaciones contienen una serie de definiciones que tienen por finalidad incorporar el lenguaje técnico propio del mundo de la electrónica al mundo del derecho. Se mencionará algunos de esos términos con el objeto de hacer más comprensible la lectura de este trabajo⁵²:

-Criptografía: rama de las matemáticas aplicadas que se ocupa de transformar mensajes en forma aparentemente ininteligibles y devolverlos a su forma original.

-Criptosistema asimétrico: algoritmo o serie de algoritmos que brindan un par de claves seguras. Utiliza un par de claves compuestas por una clave privada, empleada para firmar digitalmente y su correspondiente clave pública, usada para verificar esa firma digital, de forma tal, que con las longitudes de claves utilizadas, sea

⁵² Tomados del Proyecto sobre Comercio Electrónico de Del Piero-Molinari y de la página oficial de Infraestructura de Firma Digital de la República Argentina “www.pki.gov.ar”

computacionalmente no factible tanto obtener o inferir la clave privada a partir de la correspondiente clave pública como desenscriptar aquello que ha sido encriptado con una clave privada, sin la utilización de la correspondiente clave pública.

-Par de claves: clave privada y su correspondiente clave pública en un criptosistema asimétrico seguro.

-Clave privada: clave que se utiliza para firmar digitalmente, mediante un dispositivo de creación de firma digital, en un criptosistema asimétrico seguro. Es una familia de métodos matemáticos –algoritmos- que admite distintas implementaciones tanto en hardware como en software.

-Clave pública: clave que se utiliza para verificar una firma digital, en un criptosistema asimétrico seguro. Es una familia de métodos matemáticos –algoritmos- que admite distintas implementaciones tanto en hardware como en software.

-Clave Secreta: dentro de un Criptosistema de Clave Secreta (o Criptosistema Simétrico), es la clave secreta compartida entre los participantes de una comunicación en el contexto de un Criptosistema Simétrico, utilizada en los procesos de encriptación y desenscriptación de datos.

-Función Hash (message digest function): función de transformación matemática que asocia valores de un dominio extenso a uno de menor rango. Las funciones de hash tienen las siguientes características: (1) son funciones unidireccionales (a partir del resultado de la aplicación de una función hash, es imposible volver a recuperar la entrada inicial), (2) están libre de colisiones (dadas dos entradas diferentes, no se puede obtener el mismo resultado de aplicación de función hash), (3) son funciones aplicables a bloques de cualquier tamaño, (4) originan siempre un resultado de tamaño fijo y considerablemente menor al de la entrada, (5) son relativamente sencillas de calcular para cualquier entrada.

-Función Unidireccional: función cuya inversa es computacionalmente imposible de calcular.

-Camino de Certificación: secuencia ordenada de certificados digitales. La relación que rige la ordenación de la secuencia se basa en la siguiente propiedad: dado un certificado de una entidad determinada, el siguiente certificado en la secuencia corresponde al asociado a la Autoridad de Certificación que emitió el certificado del usuario anterior.

-CBC (Cipher Block Chaining): método de utilización de un esquema de encriptación de bloques para encriptar un mensaje de tamaño arbitrario.

-Certificado de Clave Pública: unidad de datos firmada digitalmente por una Tercera Parte Fiable o Autoridad de Certificación, que asocia una clave pública a un identificador de entidad propietaria de dicha clave. El certificado digital contiene el identificador del propietario del certificado, la clave pública que está certificando, información adicional como identificadores de algoritmos, nombres alternativos o usos de claves, y por último la entidad que emite el certificado añade la firma digital de la información citada. Por el hecho de estar firmados digitalmente (cifrados con la clave privada) por una Tercera Parte Fiable, estos certificados son por sí mismos seguros e infalsificables, pudiéndose transmitir estos mediante redes inseguras y utilizando protocolos no dotados de medidas de seguridad. La función principal de los certificados digitales es probar la identidad de los propietarios de los mismos.

-CFB (Cipher Feedback Chaining): método utilizado en un esquema de encriptación de bloques para encriptar mensajes de tamaño arbitrario.

-Checksum: pieza de datos de longitud fija y pequeña, función de un mensaje de tamaño arbitrario. Un checksum se calcula en la parte del generador del mensaje, y se vuelve a computar y se chequea en la parte receptora del mensaje con el fin de detectar corrupción de datos. Originalmente, el término checksum significaba un chequeo específico de integridad que consistía únicamente en la transmisión del mensaje original junto con la adición de una secuencia de dígitos función de este mensaje. El uso del checksum ha ampliado su definición para incluir funciones adicionales complejas criptográficas y no criptográficas, tales como digest de mensajes que detectan fallos del hardware ocurridos con una probabilidad alta y funciones criptográficas tales como

CRCs, las cuales soportan ataques de agentes maliciosos sobre datos transmitidos en una comunicación electrónica.

-CPS(Certificate Practice Statement): sentencias detalladas de prácticas y procedimientos operacionales que una Autoridad de Certificación emplea en la emisión de certificados.

-Criptoanálisis: parte de la criptografía que concierne a la decodificación de mensajes encriptados por parte de agentes no autorizados a obtener dichos datos en claro.

-Condiciones de emisión y utilización de los certificados: documento que emite la autoridad certificante y que contiene los términos de emisión de sus certificados.

-Dispositivo de creación de firma: conjunto de hardware o software, técnicamente confiable, que permite que los datos utilizados para la generación de la firma digital no sean deducidos o derivados de la propia firma y puedan producirse sólo una vez, y que asegura razonablemente su secreto.

-Dispositivo de verificación de firma digital: dispositivo de hardware o software técnicamente confiable que verifica una firma digital utilizando la clave pública del firmante.

-Soporte: modo en el cual se almacena la información de un documento digital, tal como memoria electrónica, disco magnético, magneto-óptico u óptico, cinta magnética, tarjeta inteligente, microchip.

-Ente licenciante: organismo que otorga las licencias a las autoridades certificantes.

-Autoridad certificante: tercero confiable que firma el certificado de clave pública y pone en conocimiento público los certificados.

-**Signatario:** persona física que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa.

-**Computacionalmente no factible:** cualidad de aquellos cálculos matemáticos asistidos por computadora que, para ser llevados a cabo, requieren un tiempo y unos recursos informáticos tales que superan ampliamente los disponibles al momento de efectuar dichos cálculos.

-**Técnicamente confiable:** cualidad del conjunto de equipos de computación, software, protocolos de comunicación y de seguridad y procedimientos administrativos relacionados, en tanto aquél reúna los siguientes requisitos: a) ser confiable para resguardar contra la posibilidad de intrusión o de uso no autorizado; b) brindar disponibilidad, confiabilidad, confidencialidad y correcto funcionamiento; c) ser apto para el desempeño de sus funciones específicas; d) cumplir con requisitos de seguridad apropiados, acordes a estándares internacionales en la materia; e) cumplir con los estándares tecnológicos que al efecto dicte la autoridad de aplicación.

-**Infraestructura de firma digital:** conjunto de leyes, normativa legal complementaria, obligaciones legales, hardware, software, bases de datos, redes, estándares tecnológicos y procedimientos de seguridad que permiten que distintas entidades (individuos u organizaciones) se identifiquen entre sí de manera segura al realizar transacciones en redes. Esta definición es conocida mundialmente con las siglas PKI que significan Public Key Infrastructure o Infraestructura de Clave Pública.

CAPÍTULO V

La firma digital en la República Argentina

El marco normativo de la República Argentina en materia de Firma digital está constituido por la ley 25506 (B.O. 14/12/2001), el Decreto 2628 (B.O. 20/12/2002) y un conjunto de normas complementarias que fijan o modifican competencias y establecen procedimientos.

A continuación se hará referencia a las principales características de los antecedentes, proyectos, informes, leyes, estándares tecnológicos y procedimientos de seguridad que forma la “infraestructura de firma digital” en Argentina.

Anteproyecto de ley de firma digital

Redactado por la Comisión Redactora del Ministerio de Justicia

Introducción a la firma digital.

Las redes abiertas como Internet revisten cada vez mayor importancia para la comunicación mundial. Esas redes permiten una comunicación interactiva entre interlocutores que no necesariamente han entablado previamente relación alguna. Además, ofrecen nuevas posibilidades empresariales, creando herramientas que mejoran la productividad y reducen los costos, así como nuevas formas de llegar al cliente. También las administraciones públicas las utilizan en su gestión interna y en su interacción con empresas y ciudadanos. El comercio electrónico brinda al país una excelente oportunidad para avanzar en su integración económica con las naciones del resto del mundo.

Para aprovechar todas estas posibilidades es necesario disponer de un entorno seguro en relación con la autenticación digital.

Beneficios de la firma digital

Al facilitar la autenticación a distancia entre partes que no necesariamente se conocen previamente, las firmas digitales constituyen el mecanismo esencial para proveer seguridad y desarrollar la confianza en las redes abiertas. Por ello constituyen un elemento clave para el desarrollo del comercio electrónico en Internet.

El comercio electrónico no es el único beneficiario de la firma digital: Actualmente las empresas y los organismos públicos de nuestro país están atorados de grandes cantidades de documentos en soporte papel que ocupan un significativo y costoso espacio de archivo en sus oficinas y que dificultan su organización, resultando en un acceso a la información mas lento y costoso.

La firma digital

El mecanismo de firma digital debe ser criptográfico, pues si lo que se desea es proteger la información, o sea los dígitos, se incursiona necesariamente en el campo de la criptografía, la que se define como el arte de proteger la información, tanto como para proteger su privacidad como para proteger su integridad. El término criptografía proviene del griego (cripto: oculto) y es definido por el diccionario de la Real Academia como el "arte de escribir con clave secreta o de un modo enigmático" (Diccionario de la Lengua Española, Real Academia Española, vigésimo primera edición, Tomo I, pág. 596, Madrid, 1992).

No se dice que el mecanismo de firma digital deba ser únicamente criptográfico, sino meramente que la criptografía forma parte esencial sine qua non de ese mecanismo de firma digital, pudiendo intervenir en el proceso de firma otros mecanismos tales como los mecanismos biométricos, pero sólo en forma adicional a la criptografía.

Resta hallar entonces la condición que permita identificar al creador de una firma digital, teniendo en cuenta que cualquier cualidad manifiesta a simple vista puede ser fácilmente copiada y transferida de un documento a otro.

La condición buscada está disponible y consiste en el secreto no compartido. Este mecanismo existe y en el ámbito de la criptografía se denomina criptografía asimétrica o criptografía de clave pública

Enfoques y principios legislativos

Es importante destacar que este Anteproyecto de Ley no hace obligatoria la utilización de la firma digital en desmedro de la manuscrita, sino que tal utilización es simplemente voluntaria. Tampoco se pretenden alterar las restantes formas de los diversos actos jurídicos y notariales, sino que como modesto objetivo se propone que un documento digital firmado digitalmente no carezca de validez jurídica únicamente por la naturaleza digital de su soporte y de su firma. Esto significa que el presente Anteproyecto respeta las restantes formas documentales existentes y que, por ejemplo, si una norma requiere en forma expresa que un documento sea manuscrito con firma manuscrita, o que se registre en un protocolo notarial, entonces no podrá aplicársele el mecanismo de firma digital al que se hace referencia en el presente Anteproyecto.

Principios y objetivos del anteproyecto de Firma Digital

- **Funcionamiento de las Firmas Digitales.** El presente Anteproyecto de Ley apunta a asegurar el buen funcionamiento de las firmas digitales, instituyendo un marco jurídico homogéneo y adecuado para el uso de estas firmas en el país y definiendo un conjunto de criterios que constituyen los fundamentos de su validez jurídica.

- **No Discriminación del Documento Digital Firmado Digitalmente.** Este Anteproyecto de Ley implementa un marco jurídico Nacional que garantiza que la fuerza ejecutoria, el efecto o la validez jurídica de una firma digital no sea cuestionado por el solo motivo de que la firma se presenta bajo la forma de datos digitales.

- **Libertad contractual.** La tecnología de firmas digitales tiene aplicaciones evidentes en entornos cerrados, como ser la red local de una empresa o un sistema bancario. Los certificados de clave pública y las firmas digitales tienen igualmente una función de autorización, por ejemplo para acceder a una cuenta personal. En el marco de la legislación nacional, el principio de la libertad contractual permite a las partes contrayentes convenir entre ellas la modalidad de sus transacciones, es decir, si ellas

aceptan o no las firmas digitales. En este caso, no se manifiesta una necesidad evidente de legislación.

- No obligación de obtener Licenciamiento No Obligatorio. Teniendo en cuenta la gama de servicios en cuestión y sus posibles aplicaciones, los certificadores de clave pública prestatarios de servicios de certificación pueden ofrecer sus servicios sin la obligación de obtener una licencia. De todos modos, estos prestatarios de servicios pueden optar por beneficiarse de la validez jurídica que le confiere a las firmas digitales el régimen voluntario de licenciamiento de ésta ley.

- Otros Servicios de Certificación Relacionados a las Firmas Digitales. Un certificador de clave pública prestatario de servicios de certificación puede ofrecer una amplia gama de servicios. El presente Anteproyecto de Ley se centra particularmente en los servicios de certificación relacionados con las firmas digitales. Los certificados pueden utilizarse con fines muy diversos y contener diferentes datos. Puede tratarse de identificadores clásicos, como ser el nombre, la dirección, el número de documento de identidad, el número de contribuyente o de identificación fiscal o cualquier atributo específico del firmante, por ejemplo, que permiten establecer si está facultado para actuar en nombre de una empresa, si es solvente, si tiene garantes o si es titular de permisos o de licencias particulares. Como consecuencia, se puede visualizar la emisión de diversos tipos de certificados para múltiples usos.

- Criterio de proporcionalidad. El reconocimiento jurídico de firmas digitales debe reposar sobre criterios objetivos, transparentes, no discriminatorios y proporcionales, que no deben ser condicionados a ninguna autorización o licenciamiento del prestatario del servicio respectivo. Las exigencias comunes aplicables a los prestatarios de servicios de certificación deben permitir el reconocimiento internacional de firmas y certificados para los países del Mercosur y del mundo que cuentan con un marco normativo compatible.

- Responsabilidad. En materia de responsabilidad, las reglas comunes deben contribuir a suscitar la confianza de los usuarios y de los suscriptores y de las organizaciones, que confían en los certificados y en los prestatarios de servicios y promover así una amplia difusión de las firmas digitales.

- Operación Internacional Reconocimiento de Certificados Emitidos en Otros Países. Los mecanismos cooperativos y un marco normativo compatible que

permitan el reconocimiento entre países de las firmas y de los certificados, son esenciales para el desarrollo del comercio electrónico internacional.

Necesidad de compatibilización:

Es imprescindible que el marco legal y técnico que adopte el país para el desarrollo de la firma digital sea compatible con el que ya existe en otros países. La aplicación de criterios legales diferentes a los aplicables en otros países en cuanto a los efectos legales de la firma digital, y cualquier diferencia en los aspectos técnicos en virtud de los cuales las firmas digitales son consideradas seguras, resultará perjudicial para el desarrollo futuro del comercio electrónico nacional y, por consiguiente, para el crecimiento económico del país y su incorporación a los mercados internacionales, cada vez más globalizados.

Estándares Internacionales

La criptografía de clave asimétrica, también denominada criptografía de clave pública, forma parte de los siguientes estándares internacionales:

-ISO 9796:

International Standards Organization ("Organización de Estándares Internacionales"), Norma ISO 9796 de Tecnología de la Información – Técnicas de Seguridad – Mecanismo de Firma Digital ("Information Technology - Security Techniques - Digital Signature Scheme").

-ANSI X9.31:

Instituto Americano de Estándares Nacionales ("American National Standards Institute"), estándar X9.31 de Autenticado de Mensajes para Instituciones Financieras ("Financial Institution Message Authentication") para el sistema bancario estadounidense.

-ITU-T X.509:

Unión Internacional de Telecomunicaciones, Sector de Estandarización de Telecomunicaciones ("International Telecommunication Union, Telecommunication Standardization Sector"), estándares X.509 de Tecnología de la Información – Interconexión de Sistemas Abiertos – El Directorio: Marco para el Autenticado

("Information Technology - Open Systems Interconnection - The Directory: Authentication Framework")

-PKCS:

Estándares de Criptografía de Clave Pública ("Public Key Cryptography Standards") desarrollados por RSA Corporation en forma conjunta con Apple, Microsoft, Digital, Lotus, Sun y Massachusetts Institute of Technology.

-SWIFT:

Sociedad para las Telecomunicaciones Financieras Interbancarias Mundiales ("Society for Worldwide Interbank Financial Telecommunications")

-ETEBAC:

Sistema Financiero Francés, estándar 5.

Antecedentes internacionales

En el plano internacional existen actualmente múltiples normativas en torno a los aspectos legales de la firma digital:

- la Comisión Europea ha redactado su borrador final de Directiva de Firma Digital ("Propuesta de Directiva del Parlamento Europeo y el Consejo sobre un Marco Común Para las Firmas Electrónicas") del 13 de mayo de 1998, publicado en el Diario Oficial de las Comunidades Europeas del 23 de octubre de 1998, que establece las pautas para la utilización de la firma digital por los Estados miembros.

- la Comisión de las Naciones Unidas para el Derecho Comercial Internacional (UNCITRAL) ha aprobado una Ley-Modelo sobre Comercio Electrónico y ha comenzado a trabajar en la preparación de normas uniformes en materia de firma digital.

- la Organización de Cooperación y Desarrollo Económico (OCDE) prosigue sus trabajos en este ámbito, a modo de continuación de sus pautas de política criptográfica de 1997. Otras organizaciones internacionales, como la Organización Mundial del Comercio (OMC), han empezado también a interesarse en el tema.

- el Comité de Seguridad de la Información de la Sección de Ciencia y Tecnología de la American Bar Association ("ABA" – Asociación de Abogados de los EE.UU.) redactó su Normativa de Firma Digital en 1996, en la que especifica un

mecanismo de firma digital sobre la base de la critpografía asimétrica, los certificados de clave pública y los certificadores de clave pública.

Antecedentes Nacionales

Decreto N° 427/98 del PODER EJECUTIVO - Firmas Digitales para la Administración Pública Nacional.

Autoriza el empleo de la firma digital en la instrumentación de los actos internos del Sector Público Nacional, que no produzcan efectos jurídicos individuales en forma directa. La firma digital tiene los mismos efectos de la firma manuscrita, siempre que se hayan cumplido los recaudos establecidos y dentro del ámbito de aplicación en el Sector Público Nacional, dentro del cual se comprende la administración centralizada y la descentralizada, los entes autárquicos, las empresas del Estado, las Sociedades del Estado, las Sociedades Anónimas con participación estatal mayoritaria, los bancos y entidades financieras oficiales y todo otro ente, cualquiera sea su denominación o naturaleza jurídica, en que el Estado Nacional o sus organismos descentralizados tengan participación suficiente para la formación de sus decisiones. La correspondencia entre una clave pública, elemento del par de claves que permite verificar una firma digital, y el agente titular de la misma, se acredita mediante un certificado de clave pública emitido por un certificador de la misma. Se establecen los requisitos y condiciones para la vigencia y validez de los certificados de clave pública (emisión, aceptación, revocación, expiración y demás contingencias del procedimiento), así como las condiciones bajo las cuales deben operar los certificadores de clave pública licenciados integrantes de la citada Infraestructura de Firma Digital para el Sector Público Nacional.

Resolución MTSS N° 555/97 MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL
Normas y Procedimientos para la Incorporación de Documentos y Firma Digital.

Define el documento digital, la firma digital, el certificador de clave pública, el certificado, la clave privada, la clave pública y establece que los documentos digitales se considerarán válidos y eficaces, surtiendo todos los efectos legales y probatorios cuando estén firmados digitalmente.

Resolución SAFJP N° 293/97 SUPERINTENDENCIA DE ADMINISTRADORAS DE FONDOS DE JUBILACION Y PENSIONES - Incorporación del Correo Electrónico con Firma Digital.

Establece que los CD-ROMs remitidos por las Administradoras de Fondos de Jubilaciones y Pensiones, debidamente identificados por el Sistema, serán válidos y eficaces, surtiendo todos los efectos legales y probatorios, a partir de la fecha y hora en que queden disponibles en las bandejas de entrada y que la firma electrónica o clave de seguridad habilitante para acceder al sistema poseerá el mismo valor legal que la firma manuscrita.

Resolución SFP N° 45/97 SECRETARIA DE LA FUNCION PUBLICA - Incorporación de Tecnología de Firma Digital a los Procesos de Información del Sector Público.

La SECRETARIA DE LA FUNCION PUBLICA adhiere y hace suyos los conceptos vertidos por el Sub-Comité de Criptografía y Firma Digital del CUPI en el documento "Pautas Técnicas en la Materia de Normativa de Firma Digital" y autoriza el empleo de ésta tecnología para la promoción y difusión del documento y la firma digitales en el ámbito de la Administración Pública Nacional.

Resolución SFP N° 194/98 SECRETARIA DE LA FUNCION PUBLICA - Estándares Aplicables a la Infraestructura de Firma Digital para el Sector Público Nacional del Decreto N° 427/98.

La SECRETARIA DE LA FUNCION PUBLICA dicta los estándares de homologación de algoritmos criptográficos para la Infraestructura de Clave Pública de la Administración Pública Nacional.

Resolución SFP N° 212/97 SECRETARIA DE LA FUNCION PUBLICA - Políticas de Certificación para el Licenciamiento de Autoridades Certificantes.

La SECRETARIA DE LA FUNCION PUBLICA dicta los estándares de licenciamiento y operación de las autoridades certificantes de la Administración Pública Nacional.

Ley 25.506 de Firma Digital

Sancionada: 14 de Noviembre 2001. Promulgada de Hecho: 11 de Diciembre 2001.

Capítulo I

Consideraciones generales:

Los términos “firma digital” y “firma electrónica” no poseen el mismo significado. Según el artículo 2, “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”. Mientras que la firma electrónica es aquella que carece de algunos de los requisitos legales para ser considerada como digital (art. 5).

También existe diferencia en el valor probatorio atribuido a cada uno de ellos, dado que en la firma digital existe una presunción “iuris tantum” en su favor; lo que significa que si un documento firmado digitalmente es verificado correctamente, se presume salvo prueba en contrario que proviene del suscriptor del certificado asociado y que no fue modificado (art. 7 y 8). Por el contrario, en caso de la firma electrónica, de ser desconocida la firma por su titular corresponde a quien la invoca acreditar su validez (art. 5). Asimismo, 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.

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 (art 3), existiendo exclusiones, para los cuales las disposiciones de esta ley no son aplicables, en los casos de: a) disposiciones por causa de muerte; b) actos jurídicos del derecho de familia; c) actos personalísimos en general; d) 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 (art. 4). Un documento digital también satisface los requerimientos de escritura (art. 6)

El artículo 9, establece que para que una firma digital sea considerada válida, debe haber sido creada durante el período de vigencia del certificado digital válido del firmante; ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente; y que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado.

Capítulo II

De los certificados digitales:

Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular (art. 13).

Para ser considerados 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.

El certificado digital tiene un período de vigencia para ser considerado válido, que comienza desde su fecha de inicio y culmina en su vencimiento o revocación (art. 15).

Existe reconocimiento de los certificados extranjeros en los mismos términos y condiciones de la ley (art.16) 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, o

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.

Capítulo III

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 (art. 17). A partir de noviembre de 2003 las funciones del ente licenciante son cumplidas por la Oficina Nacional de Tecnologías de Información (Decreto N° 1028 /03).

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.

El artículo 19, establece que las funciones del certificador licenciante son:

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.

Son obligaciones del certificador licenciado (art. 21):

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.

El certificador licenciado cesa en su calidad de tal, por decisión unilateral comunicada al ente licenciante; por cancelación de su personería jurídica; por cancelación de su licencia dispuesta por el ente licenciante. La autoridad de aplicación determinará los procedimientos de revocación aplicables en estos casos (art. 22).

Capítulo IV

Del titular de un certificado digital:

El titular de un certificado digital tiene los siguientes derechos (art. 24):

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.

Son obligaciones del titular de un certificado digital (art 25):

- 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.

Capítulo V

De la organización institucional:

El artículo 27, establece que 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.

Con la misma se crea en el ámbito jurisdiccional de la Autoridad de Aplicación, la Comisión Asesora para la Infraestructura de Firma Digital (art. 28). (Por art. 8° del Decreto N° 624/2003 B.O. 22/8/2003 se establece que la Comisión creada por el presente artículo actuará en la órbita de la SUBSECRETARIA DE LA GESTION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS.)

Capítulo VI

De la autoridad de aplicación:

La autoridad de aplicación de la presente ley será la Jefatura de Gabinete de Ministros, y tendrá las siguientes funciones (art. 29 y 30):

- 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.

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 (art. 31).

Además, la autoridad de aplicación podrá cobrar un arancel de licenciamiento para cubrir su costo operativo y el de las auditorías realizadas por sí o por terceros contratados a tal efecto (art. 32).

Capítulo VII

Del sistema de auditoría:

El ente licenciante y los certificadores licenciados, deben ser auditados periódicamente, de acuerdo al sistema de auditoría que diseñe y apruebe la autoridad de aplicación (art. 33), pudiendo realizarlo por sí o por terceros como Universidades, organismos científicos y/o tecnológicos nacionales o provinciales, Colegios y Consejos profesionales que acrediten experiencia en la materia (art. 34).

Capítulo VIII

De la Comisión Asesora para la Infraestructura de Firma Digital:

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. Serán designados por el Poder Ejecutivo por un período de cinco (5) años renovables por única vez (art. 35).

Las funciones de la Comisión asesora se encuentran establecidas en el art. 36 de la norma. De acuerdo a ello emitir recomendaciones por iniciativa propia o a solicitud de la Autoridad de Aplicación, en aspectos relativos a estándares tecnológicos, el sistema de registro de la información sobre la emisión de certificados, el sistema de auditoría y otros que le sean requeridos. Asimismo deberá consultar periódicamente mediante audiencias públicas a las cámaras empresarias, los usuarios y las asociaciones de consumidores respecto a aspectos relativos al uso de la firma digital en nuestro país.

Para la conformación de la comisión, en el mes de Setiembre de 2003, la Jefatura de Gabinete de ministros invitó por nota a Universidades Públicas y Privadas, Colegios Profesionales, Cámaras y otros entes representativos de profesionales a presentar propuestas de especialistas que cumplieran con los requisitos mencionados. Luego de un proceso de selección y a través del Decreto N° 160/2004 (Boletín Oficial del 6/2/2004), el Poder Ejecutivo Nacional designó a los integrantes de la comisión asesora para la Infraestructura Nacional de Firma Digital resultando elegidos:

- Dr. Daniel Altmark (a propuesta del Colegio Público de Abogados de la Capital Federal y de la Universidad de Buenos Aires)
- Ing. Cristian Jensen (a propuesta del Ministerio de Justicia, Seguridad y Derechos Humanos)
- Escribano Agustín Sáenz (a propuesta del Consejo Federal del Notariado Argentino)
- Lic. Gabriela Brusa (a propuesta del Gobierno de la Provincia de Santa Fe)

- Lic. Armando Carratalá (a propuesta de la Cámara de Informática y Comunicaciones de la República Argentina)
- Ing. Guido Vasallo (a propuesta de la Universidad CAECE)
- Ing. Juan Aquerreta (a propuesta de la Cámara Argentina de Bases de Datos y Servicios en Línea)

En el mes de Julio de 2004, la Jefatura de Gabinete de Ministros, por medio de la Resolución 435/2004, aprueba el Reglamento de funcionamiento de la Comisión.

Capítulo IX

Responsabilidad:

Según el artículo 37, 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.

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 (art. 18).

No son responsables en los siguientes casos (art 38):

- 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.

Capítulo X

Sanciones:

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 (art. 40)

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 (art. 41)

Capítulo XI

Disposiciones Complementarias:

El Estado nacional, dentro de las jurisdicciones y entidades comprendidas en el artículo 8° 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 (art. 48).

Infraestructura de Firma Digital

La misma está conformada por:

-Autoridad de aplicación: Es la Jefatura de Gabinete de Ministros, quién está facultada a establecer las normas y procedimientos técnicos necesarios para la efectiva implementación de la ley.

Por medio del Decreto 1028/03 la Oficina Nacional de Tecnologías de Información (ONTI) también está facultada para definir las normas y procedimientos reglamentarios del régimen de Firma Digital.

-Comisión Asesora para la Infraestructura de Firma Digital: Funciona en el ámbito de la Subsecretaría de la Gestión Pública, emitiendo recomendaciones sobre aspectos técnicos referidos al funcionamiento de la Infraestructura de Firma Digital.

A través del Decreto 160/2004, el Poder Ejecutivo Nacional ha designado a los integrantes de la Comisión Asesora para la Infraestructura Nacional de Firma Digital, en cumplimiento con lo dispuesto en la ley 25506.

-Ente Licenciante: Es el órgano técnico-administrativo encargado de otorgar las licencias a los certificadores y de supervisar su actividad. Funciona en el ámbito de la Oficina Nacional de Tecnologías de Información (ONTI).

-Certificadores licenciados: Son aquellas personas de existencia ideal, registro público de contratos u organismo público que obtengan una licencia emitida por el ente administrador para actuar como proveedores de servicios de certificación en los términos de la ley 25506 y su normativa complementaria.

-Autoridades de registro: Son entidades que tienen a su cargo las funciones de validación y otros datos de los suscriptores de certificados. Dichas funciones son delegadas por el certificador licenciado.

-Sistema de Auditoría: Será establecido por la autoridad de aplicación, a fin de evaluar la confiabilidad y calidad de los sistemas utilizados por los certificadores licenciados.

Este marco normativo deroga el Decreto 427/98, cuya aplicación era específica para el Sector Público, por cuanto cubre sus objetivos y alcance.

Régimen normativo vigente en la República Argentina

- Ley 25506 de Firma Digital – Boletín Oficial del 14/12/2001.
- Decreto N° 2628/2002: Reglamenta la Ley N° 25506 de firma digital. Crea el Ente Administrador de Firmas Digitales.
- Decreto N° 1028/2003: Disuelve el Ente Administrador de Firma Digital, creado por el artículo 11 del Decreto N° 2628/02, cuyo accionar será llevado a cabo por la Oficina Nacional de Tecnologías de Información de la Subsecretaría de la Gestión Pública (ONTI). El mismo debe promover la estandarización tecnológica en materia informática, teleinformática o telemática y telecomunicaciones; entender en el marco regulatorio del régimen relativo a la validez legal del documento y firma digital; ejercer las funciones de Autoridad Certificante de firma digital para el Sector Público Nacional; proponer y mantener actualizados los estándares sobre tecnologías en materia informática y telecomunicaciones; mantener el Portal General del gobierno de la República Argentina; solicitar los informes de auditoría y realizar inspecciones a los certificadores licenciados de Firma Digital.
- Decreto N° 160/2004: Designa los integrantes de la Comisión Asesora para la Infraestructura Nacional de Firma Digital, en cumplimiento de lo dispuesto en la Ley N° 25506.

- Resolución JGM N° 435/2004: Aprueba el Reglamento de funcionamiento de la Comisión Asesora para la Infraestructura de Firma Digital, creado por la Ley N° 25506 y designados por el Decreto N° 160/2004 del Poder Ejecutivo Nacional.

El mismo establece, entre otros, que se designará entre sus miembros un Coordinador General y un Secretario, quienes ejercerán tales funciones por un período de seis meses; la Comisión se reunirá en cada oportunidad que lo solicite la Subsecretaría de la Gestión Pública o cuando uno o varios de sus miembros lo consideren oportuno, en donde se deberá elaborar un acta; adoptará sus decisiones, por simple mayoría de adhesiones de los miembros presentes y con un quórum mínimo de 4 (cuatro) miembros; por cada tema tratado o sometido a su consideración, la Comisión deberá elaborar un dictamen que elevará a la Subsecretaría de la Gestión Pública.

- Decreto N° 152/2003: Otorga competencia a la Subsecretaría de la Gestión Pública para licenciar a los certificadores, supervisar su actividad y dictar normas tendientes a asegurar el régimen de libre competencia en el marco de los prestadores y protección de los usuarios de firma digital.

- Decreto N° 283/2003: Autoriza con carácter transitorio a la Oficina Nacional de Tecnologías de Información a proveer certificados digitales para su utilización en aquellos circuitos de la Administración Pública Nacional que requieran firma digital, de acuerdo a la Política de Certificación vigente.

- Decreto N° 1023/2001: En su artículo 21 permite la realización de contrataciones comprendidas en el Régimen en formato digital firmado digitalmente. También podrán realizarse en formato digital firmado digitalmente los contratos previstos en el artículo 5° del presente: a) los de empleo público; b) las compras por caja chica; c) los que se celebren con estados extranjeros, con entidades de derecho público internacional, con instituciones multilaterales de crédito, los que se financien, total o parcialmente, con recursos provenientes de esos organismos; d) los comprendidos en operaciones de crédito público.

Las jurisdicciones y entidades comprendidas en el artículo 2° (entidades del art. 8 de la Ley 24156) estarán obligadas a aceptar el envío de ofertas, la presentación de

informes, documentos, comunicaciones, impugnaciones y recursos relativos a los procedimientos de contratación establecidos en este régimen, en formato digital firmado digitalmente, conforme lo establezca la reglamentación.

Los documentos digitales firmados digitalmente tendrán el mismo valor legal que los documentos en soporte papel con firma manuscrita, y serán considerados como medio de prueba de la información contenida en ellos.

- Resolución SFP N° 194/98: Establece los estándares sobre tecnología de firma digital para la Administración Pública Nacional.

Normativa sobre Firma Digital específica para el Sector Público

En el caso particular de la Administración Pública Nacional, se encuentra vigente el Decreto N° 283/03, que autoriza con carácter transitorio a la Oficina Nacional de Tecnologías de Información a proveer certificados digitales para su utilización en aquellos circuitos de la Administración Pública Nacional que requieran firma digital, de acuerdo a la política de certificación vigente.

Este decreto es de aplicación transitoria hasta tanto se encuentre la Administración Pública Nacional en condiciones de emitir certificados digitales en los términos previstos en la Ley 25506 y establece además un puente entre el marco normativo creado por el Decreto 427/98 (derogado por el Decreto 2628/02) y el marco normativo establecido por la citada Ley.

Normativa sobre aplicaciones en el Sector Público

Independientemente del marco normativo general existente para el Sector Público, distintos organismos han establecido procedimientos o aplicaciones específicas para sus operaciones internas, o para las comunicaciones que establecen con sus administrados que habilitan el uso de documentos electrónicos y firmas digitales.

A continuación se detallan algunas normas relacionadas con la utilización de Documentos Electrónicos y Firma Digital en el Sector Público:

- Resolución del Min. Interior N° 618/2004: Crea el Programa de Transparencia de las Contrataciones en el ámbito del Ministerio del Interior, estableciendo que todas las comunicaciones con las Unidades Operativas de Contrataciones del Ministerio, Policía Federal, Gendarmería Nacional y Prefectura Naval se harán en formato digital firmado digitalmente.
- Resolución Secretaría de Hacienda N° 24/04: Habilita la utilización del correo electrónico firmado digitalmente para que las Jurisdicciones y Entidades del Artículo 8°, inciso a), b) y c) de la Ley 24156 remitan a la Subsecretaría de Presupuesto los datos generados en su sistema liquidador de haberes.
- Acordada STJ Jujuy N° 70/2002: Autoriza el uso de la firma digital para comunicaciones que materialicen trámites judiciales entre organismos jurisdiccionales provinciales y trámites administrativos y judiciales entre organismos jurisdiccionales provinciales y los de otras provincias.
- Resolución Administrativa STJ Chubut N° 508/02: Autoriza la realización de una experiencia piloto de notificación por cédula en dirección de correo electrónico constituida al efecto, mediante cédula emitida a través de correo electrónico y firmada digitalmente.
- Disposición ONTI N° 5/02: Documentación técnica de la Autoridad certificante de la Oficina Nacional de Tecnologías de Información.

Define los términos que rigen la relación entre la Oficina Nacional de Tecnologías Informáticas de la Subsecretaría de la Gestión Pública de la Jefatura de Gabinete de Ministros, en su carácter de Autoridad Certificante y sus funcionarios y agentes que soliciten la emisión de certificados de clave pública para ser utilizados en el marco del Decreto 427/98. Asimismo, regula la relación que pueda crearse entre dicha Autoridad Certificante y los funcionarios y agentes dependientes de otros organismos o dependencias de la Administración Pública Nacional Centralizada y Descentralizada, de

entes autárquicos, organismos provinciales y municipales, de otros Poderes del Estado Nacional y de los Estados Provinciales y de representantes del sector privado, a través de convenios específicos firmados en cada caso en particular.

- Resolución JGM N° 176/2002: Habilita en Mesa de Entradas de la Subsecretaría de la Gestión Pública el Sistema de Tramitación Electrónica para la recepción, emisión y archivo de documentación digital firmada digitalmente.

- Resolución SGP N° 17/2002: Establece el procedimiento para solicitar la certificación exigida al Registro del Personal acogido al Sistema de Retiro Voluntario, habilitando la modalidad de tramitación mediante el empleo de documentación digital firmada digitalmente.

- Decreto N° 677/2001: Otorga a los documentos digitales firmados digitalmente remitidos a la Comisión Nacional de Valores, de acuerdo a las reglamentaciones dictadas por ese organismo, similar validez y eficacia que los firmados en soporte papel.

- Decreto N° 103/2001: Aprueba el Plan Nacional de Modernización de la Administración Pública Nacional.

- Resolución General N° 345/99: La Comisión Nacional de Valores establece que atento al actual estado de desarrollo de las comunicaciones, es conveniente actualizar los medios por los cuales se difunden al público inversor las informaciones que le permitan adoptar más adecuadas decisiones de inversión, en particular incorporando para ello la INTERNET.

Visto el desarrollo tecnológico de la firma digital mediante el mecanismo criptográfico denominado de “Clave Pública”, de uso habitual y masivo en el comercio electrónico internacional en la INTERNET, que por su confiabilidad y seguridad torna conveniente su adopción para la informatización y despapelización de los procedimientos administrativos de la COMISION NACIONAL DE VALORES.

- Resolución SAFJP N° 293/97: Implementa en el ámbito de la Superintendencia de Administradoras de Fondos de Jubilaciones y Pensiones, el sistema de

Telecomunicaciones de la SAFJP con el fin de establecer un correo electrónico entre las Administradoras de Fondos de Jubilaciones y Pensiones y este organismo.

Subsecretaría de la Gestión Pública

Este organismo cuenta con un servicio abierto a la comunidad de Internet en la página “www.ca.sgp.gov.ar/eMail/” para todas aquellas personas que deseen contar con un Certificado Digital o Certificado de Clave Pública para firmar experimentalmente sus correos electrónicos. Esta Autoridad Certificante emite certificados de correo electrónico, por lo cual únicamente verificará la existencia y disponibilidad de la dirección de mail desde la cual se efectuó la solicitud, pero en ningún caso verificará la identidad de quien lo solicita.

Requerimientos:

Se debe tener instalado un navegador de alguna de las versiones nombradas a continuación:

- Netscape Communicator 4.03 o superior
- Internet Explorer 4.0x o superior
- Opera 5.0x o superior

Si no se cuenta con alguna de estas versiones, se puede obtener una versión actualizada a través de la página antes mencionada. Deberá tener habilitadas las opciones de JavaScript o VBScript.

También debe contar con una cuenta de correo que pueda ser utilizada desde un cliente de correo (por ejemplo Netscape Messenger o Outlook Express), las cuentas de correo de tipo webmail (por ejemplo hotmail o yahoo) no le permiten operar con esta tecnología.

Para obtener un Certificado de Clave Pública se deberá cumplimentar con los siguientes pasos:

- 1 - Instalar el Certificado de la Autoridad Certificante.
- 2 - Completar el formulario de Solicitud de Certificado.
- 3 - Recibir la confirmación de Recepción de Solicitud de Certificado.

- 4 - Esperar la recepción del Mail de Verificación.
- 5 - Realizar la confirmación solicitada en el mencionado mail.
- 6 - / Esperar la recepción del Mail de Notificación, por parte de la Autoridad Certificante, el cual le indicará como acceder a su certificado para poder retirarlo.
- 7 - / Acceder al sitio web de la Autoridad Certificante a fin de verificar la información contenida en el certificado a retirar.
- 8 - Retirar su certificado del sitio web de la Autoridad Certificante.
- 9 - - / Configurar su certificado en su Cliente de Correo para poder firmar electrónicamente.

Todos los certificados otorgados por una Autoridad Certificante son emitidos, por cuestiones de seguridad, por un período de validez determinado, vencido este período el certificado no puede ser utilizado para firmar. Sin embargo con anterioridad a la fecha de vencimiento, si el certificado no ha sido revocado, se puede renovar el certificado y extender de esa forma el tiempo de vida útil de ese certificado de manera de poder continuar utilizándolo.

Para ello se deberá cumplir con los siguientes pasos:

- 1 - Hacer la elección del método de renovación a utilizar.
- 2 - Hacer el pedido de renovación del certificado.
- 3 - Recibir la confirmación de Recepción de Solicitud de Renovación.
- 4 - Esperar la recepción del Mail de Verificación.
- 5 - Realizar la confirmación solicitada en el mencionado mail.
- 6 - Esperar la recepción del Mail de Notificación, por parte de la Autoridad Certificante, el cual le indicará como acceder a su certificado para poder retirarlo.
- 7 - Acceder al sitio web de la Autoridad Certificante a fin de verificar la información contenida en el certificado a retirar.
- 8 - Retirar su certificado del sitio web de la Autoridad Certificante.
- 9 - Configurar su certificado en su Cliente de Correo para poder firmar electrónicamente.

Existen distintas razones por las cuales se está obligado a revocar su certificado:

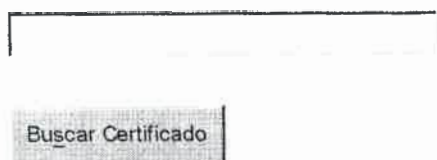
- Sospecha de que la clave privada del usuario haya sido comprometida.
- Pérdida de la clave privada que posibilita la firma.
- En caso de que el usuario decida no utilizar más ese certificado; este caso no es obligatorio pero sí recomendable.

Una vez revocado un certificado, aunque se encuentre dentro de su período de validez, éste no puede ser utilizado para firmar electrónicamente y en caso de ser utilizado para tal fin esta firma no es válida.

Para revocar el Certificado de Clave Pública se debe cumplimentar los siguientes pasos:

- 1 - Elegir el método de revocación.
- 2 - Hacer el pedido de revocación del certificado.

La mencionada página de Autoridad Certificante de la Subsecretaría de la Gestión Pública cuenta con servicios de búsqueda de certificados emitidos por esta Autoridad Certificante para instalarlos en su navegador y poder enviar mensajes encriptados a otros usuarios que posean un certificado de clave pública. Para realizar la búsqueda se debe buscar el certificado por el nombre y/o apellido con que fue emitido el certificado a esa persona y presionar el botón [Buscar Certificado]



También, la Autoridad Certificante emite la Lista de Certificados Revocados la cual contiene todos los certificados que por algún motivo han sido revocados por su titular o por esta autoridad.

Se puede instalar en su cliente de correo esta lista de revocación, de esta forma cada vez que reciba un e-mail firmado, su navegador verificará contra esta lista que el certificado del remitente no este revocado y sea válido a pesar de que se encuentre el mismo dentro de su período de validez.

Para instalar la Lista de Revocación debe hacer click en el link que dice [Instalar Lista de Revocaciones]. Aparecerá la ventana "Descarga de archivos". Seleccione "Guardar este archivo a disco", puede guardarlo en su escritorio o en el disco raíz C:

Si se guardó el archivo en el escritorio podrá verlo fácilmente, si en cambio lo guardó en algún directorio se tendrá que trasladar con el explorador hasta el mismo. Una vez visualizado el archivo con el botón derecho del mouse haga click sobre el archivo, seleccione la opción "Instalar CRL".

Aparecerá un conjunto de pantallas estilo asistente donde se detallarán los pasos que está realizando sólo necesita presionar [Siguiente] y [Finalizar]. Finalmente aparecerá un cuadro de diálogo que le avisará que la importación se realizó con éxito.

Si se desea firmar digitalmente un correo electrónico, se debe proceder de la siguiente forma:

1. Abrir el programa que utiliza para enviar sus correos electrónicos. Se sigue con el procedimiento habitual para escribir el mensaje que desea enviar y a continuación, se efectúa los pasos que se indican según el cliente de correo que utilice:

Si utiliza Netscape Navigator:

2. Presione el botón de Opciones (Options) y haga click en la casilla de verificación Firmado (Signed).

Si utiliza Outlook Express:

2. En el extremo derecho de la segunda fila de instrucciones observará dos iconos similares. Haga un click en el que representa un sobre con una "cinta roja" o se puede ir al menú de Herramientas (Tools) y luego ir a Firmar mensaje digitalmente (Digitally Sign).

3. Presione el botón Enviar

4. Por último, ingrese su palabra clave a fin de firmar el mensaje y luego haga un click en Aceptar para enviar el mensaje firmado.

Conclusión

Las principales dificultades que se observan en el estudio de la firma digital y los documentos electrónicos, es la creencia de que el documento está inexorablemente unido a la documentación escrita y que la única evidencia certera de la autoría es la firma holográfica.

Esta es una regla admitida y difundida en la mayoría de las legislaciones. Regla que se extendió en su aplicación porque hubo una difusión de los presupuestos tecnológicos que la hicieron viable: el uso del papel y posteriormente la imprenta.

Por lo que, resulta obvio, que si disminuye el uso del papel surgirán otras herramientas jurídicas que le den respuesta a los cambios.

Con el uso de la tecnología digital se han difundido nuevas formas de relaciones jurídicas, surgiendo inconvenientes que deben ser resueltos.

El uso del documento electrónico plantea una cuestión de reconocibilidad, es decir, en qué condiciones existe un documento y cuando es atribuible a su autor. Todos los problemas que surgen de la contratación electrónica se relacionan con el asiento de la declaración de voluntad, es decir, con el traslado de una documentación corporal hacia una incorporeal.

No se trata de un nuevo sistemas de reglas y funciones del mundo digital, de lo que se trata es de garantías. Precisar si los bits ofrecen seguridad suficiente para cumplir con las funciones del documento en soporte papel y de la firma holográfica.

Lo primero que se puede hacer, es establecer una analogía directa con los conceptos, técnicas y reglas de la cultura escrita a la informática.

Esto plantea inconvenientes como la imposibilidad de comparar el original y el falso para deducir su autenticidad, someterlo a pericias caligráficas, exámenes, debido a que no existen los bits falsos. Un bits hace una copia exacta de otro original.

La firma es un medio para vincular un documento con su autor. Una persona escribe debajo de un documento su nombre y apellido y se entiende que con ello declara la aceptación de la declaración de voluntad vertida en él.

Igualmente con la firma electrónica existe la intención de reconocer la autoría, pero no necesariamente mediante el nombre y apellido, y sin la escritura de mano propia. Si bien se habla de firma, se utiliza este concepto como una semejanza para

hacer más comprensible una idea. Más aún, la firma digital no ha sido pensada sobre la base de la firma tradicional. En el mundo digital, la misma no está constituida por trazos manuales del autor, sino por claves que le pertenecen de un modo indudable.

El fundamento técnico para que ello sea posible lo da la criptología, que estudia la ocultación, disimulación o cifrado de la información y los sistemas que lo permiten. Es así, como el procedimiento para la realización de una firma electrónica se denomina criptografía.

La mayoría de las legislaciones se basan en el sistema de criptografía asimétrica o de clave pública. La misma utiliza dos claves, una pública y otra privada, a diferencia de la criptografía simétrica que utiliza una sola. La clave pública es respaldada por una autoridad certificante de autoría, la clave privada es sólo atribuible al poseedor, y por lo tanto es asimilable a una firma en el sentido de que es el método más confiable para atribuir la autoría de un documento.

Si bien es cierto que en la actualidad la firma digital se basa en la criptografía de claves, relacionarlas como verdades inmutables sería cometer un grave error. La firma electrónica encontrará muchas técnicas, y a medida que éstas cambien cambiarán las leyes que se basaban en la misma.

La Argentina, con la sanción de la ley 25506 de Firma Digital en el año 2001, se colocó a la par de las legislaciones de los países más avanzados del mundo y con ello se abre toda una nueva posibilidad de integración mundial, nuevas posibilidades de crecimiento y desarrollo comercial.

La expansión de Internet y el comercio electrónico va a hacer del uso de los documentos electrónicos y la firma digital más común y, por lo tanto, una herramienta necesaria para todos aquellos con ganas de superarse y no quedarse en las viejas prácticas, quedando aislado del mundo.

Eliminar el uso del papel y automatizar los circuitos administrativos mediante la implementación de tecnología de última generación deben ser los objetivos tanto del sector privado como de la Administración Pública para comenzar el nuevo milenio de la forma más avanzada posible.

En este sentido, fue esta última, quien primero y en forma progresiva adoptó el uso de los documentos electrónicos y firma digital, incorporándolos a su sistema administrativo mediante un conjunto de resoluciones y decretos que le daban validez jurídica, lo que permitió una marcada agilización en el intercambio de información tanto interna, entre dependencias de la misma, como externa con los particulares. Este avance

no fue congruente para el sector privado, donde la falta de legislación y herramientas jurídicas han imposibilitado el desarrollo de este instrumento, haciendo que el mismo todavía se base en las viejas prácticas manuales y personales.

Si se espera que nuestro país, verdaderamente, se encuentre entre los más avanzados del mundo, es necesario una política global, donde se brinde posibilidades de desarrollo y crecimientos para todos los sectores por igual.

Espero que este trabajo haya brindado el conocimiento necesario para la utilización de los documentos electrónicos y la firma digital para el común de la gente. Con esto hago referencia de que el mismo no contiene las especificaciones técnicas más avanzadas para el uso de estas herramientas, pero si todo lo imprescindible.

Resumen del Trabajo Final

Los cambios de la era digital

Las sociedades humanas se caracterizan por el constante cambio que causan una profunda incidencia en el desarrollo de patrones de conducta social, creando entre las personas nuevos modos de interacción.

La revolución tecnológica ha redimensionado las relaciones entre los hombres, al punto tal, de que se la considera la figura representativa de nuestra cultura, muchas veces denominada “sociedad de la información”.

El fin de siglo, se vio caracterizado por una convergencia de tecnología hasta el momento independiente. Esta convergencia que experimenta la Electrónica, la Informática y las Telecomunicaciones, tiene su mayor exponente en el vertiginoso crecimiento alcanzado por Internet.

Internet es una red internacional o de computadoras interconectadas, que permite comunicarse entre sí a decenas de millones de personas, así como acceder a una inmensa cantidad de información de todo el mundo.

Esta tecnología no sólo actúa hoy como un importante motor del crecimiento porque a sus ventajas económicas en términos de valor añadido, productividad y empleo, se suman otras relacionadas con la posibilidad de permitir la transmisión y generalización de ventajas y experiencias entre diferentes regiones y ambientes, no sólo ignora las barreras del tiempo y el espacio ya que sus servicios están las 24 horas y en cualquier rincón del planeta, sino que también modifican las relaciones inter ciudadanos y ésta con las diferentes instituciones.

La tecnología digital produce una desestructuración en conceptos como el espacio, el tiempo o la diferencia entre público y privado que trajo como consecuencia un cambio no sólo en la forma de pensar sino en la de realizar las cosas.

Es así como existe un nuevo espacio, el cibernético, distinto del espacio físico que se caracteriza por ser autónomo, posorgánico y activo, por la existencia de una aceleración del tiempo histórico que hace que el presente se torne omnipresente y que la dimensión del pasado o del futuro se adelgacen y un creciente ascenso hacia un status

global, que permite a los sujetos comunicarse entre sí sin que sientan una presencia del Estado nacional y su marco regulatorio.

Producto de la transformación que ha generado la tecnología digital, la conceptualización de la economía ha cambiado de actores y de escenario. Tres de cada diez personas en el mundo tienen acceso directo e indirecto a Internet, generando que el mercado (lugar donde concurren compradores y vendedores), se transforme en el ciberespacio, las necesidades tradicionales continúan existiendo dentro del ciberespacio, los ofertantes y demandantes se convierten en cibernautas, y el desarrollo del comercio y sus transacciones se realizan de forma digital sin papeles.

Es una economía basada, en el cerebro y no el músculo, se evoluciona hacia una economía fundamentada en la inteligencia y en el conocimiento. En la nueva economía, los activos claves de la organización son intelectuales y se concentran en el trabajador del conocimiento.

En la antigua economía, la información era análoga o física, las personas se comunicaban al desplazar sus cuerpos físicos en un salón de reuniones, hablaban a través de una línea telefónica análoga o enviaban cartas. En la nueva economía, la información se halla en medios digitales: bits, y cuando es digitalizada y comunicada a través de redes digitales, se abre un nuevo mundo de posibilidades.

Lo masivo se convierte en molecular en todos los aspectos de la vida económica y social. La nueva empresa tiene una estructura molecular fundamentada en el individuo.

La nueva economía es una economía en red. Las redes de la nueva tecnología permiten a pequeñas compañías superar las principales ventajas (economías de escala y acceso a los recursos) de las grandes firmas al mismo tiempo que no se ven agobiadas por las principales desventajas percibidas en las grandes organizaciones: burocracia agonizante, jerarquías sofocantes e incapacidad para cambiar.

Las funciones de intermediación conocidas entre los productores y consumidores se están eliminando a través de redes digitales, pudiendo las empresas comprar o vender a través de la misma en forma directa.

Un impulsor clave en la nueva economía es la innovación, la cual constituye un compromiso con la continua renovación de productos, sistemas, procesos, mercadotecnia y personal. En la economía de innovación, la imaginación humana, es la principal fuente de valor.

En una economía basada en bits, la inmediatez se convierte en un impulsor y variable clave en la actividad económica y el éxito de las empresas. La nueva empresa es una empresa de tiempo real, la cual continua e inmediatamente se ajusta a las cambiantes condiciones de los negocios a través de la inmediatez en la información.

Los documentos electrónicos

Se podría decir en términos amplios que se entiende por documento a cualquier objeto que contiene una información que narra, hace conocer o representa un hecho, cualquiera sea su naturaleza su soporte o su continente, su proceso de elaboración o su tipo de firma.

Como la representación de hechos y actos que ocurren en la realidad puede realizarse de diferentes maneras (verbal, escrita, etc), también puede efectuarse a través del sistema eléctrico, que lo denominamos digital.

Es así como la ley 25506 en su artículo 6 define al documento digital como una representación digital de hechos y actos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo: esto es eléctrico, magnético, óptico, etc.

Los documentos electrónicos poseen los mismos elementos que un documento escrito en soporte papel: un soporte material (cintas, diskettes, circuitos, chips de memoria, redes); contiene un mensaje, el que está escrito usando el lenguaje convencional de los dígitos binarios o bits; están escritos en un idioma o código determinado; pueden ser atribuidos a una persona determinada en calidad de autor mediante una firma digital, clave o llave electrónica.

De la palabra documento, también se distingue la palabra "instrumento" (como algo destinado a instruirnos e informarnos del pasado). En la base de la noción de documento está la idea de docencia, en el de instrumento la de prueba.

Se puede distinguir entre instrumentos públicos e instrumentos particulares, firmados o no. Los instrumentos particulares que llevan la firma del otorgante o de los otorgantes se denominan instrumentos privados.

En consecuencia con los avances tecnológicos, se afirma que también constituyen instrumentos particulares no firmados los impresos, registros visuales o

audiovisuales de cosas o hechos y, cualquiera fuese el medio empleado, los registros de pensamientos o información, como los libros de los comerciantes, billetes de pasajes de transporte (terrestre, aéreo), tickets expedidos por cajeros automáticos.

La inserción de la firma en un instrumento público o privado permite individualizar al sujeto que la suscribe, dado su carácter habitual que implica un trazo particular. La firma insertada en un documento implica la conformidad del firmante con su contenido.

Este concepto de firma responde a un esquema tradicional donde el modo de realizarla era la escritura, y la ubicación que debía tener en el documento o instrumento signado era relevante. Sin embargo, cuando el documento es digital, ambas características pierden relevancia, adquiriendo importancia solo su función: identificar al sujeto que lo emite y considerarlo como prueba de la manifestación de su voluntad. Se agrega además la función de garantizar la inalterabilidad del documento.

En la firma electrónica, existe la intención de reconocer la autoría, pero no necesariamente mediante el nombre y el apellido, y sin la escritura de mano propia. Por lo tanto, la noción de firma es una analogía que se utiliza para hacer más comprensible una idea.

El documento electrónico puede ser firmado o no, y en ambos casos puede haber un original y un duplicado; este último puede ser legítimamente emitido por el autor o por un tercero, o bien ser una falsificación ilegítima.

La dificultad que ofrece el documento electrónico reside en que el original es igual al duplicado, ya que los bits son idénticos.

El concepto de documento original puede ser definido por las partes o por el legislador; en este último caso, la tendencia se orienta a tomar en cuenta la primera generación, en el sentido de primera elaboración.

En la Argentina existe una amplia y consolidada tendencia hacia la recepción del documento electrónico, en los campos más diversos como por ejemplo: en materia societaria, en la ley 19550, artículo 61 que establece la posibilidad de llevar ciertos libros por medio de ordenadores, medios mecánicos o magnéticos; las declaraciones en materia impositiva y previsional pueden ser efectuadas por medios informáticos en una variedad de formas que han sido autorizadas por los organismos de control (resolución SAFJP 293/1997); las acciones nominativas no endosables y escriturables pueden ser registradas en medios electrónicos (artículo 6, decreto 83/1986), y pueden prescindir de

la firma del director y del síndico si existe una impresión que garantice su autenticidad (artículo 212, ley 19550).

La firma digital

La denominada “firma electrónica” es un tema esencial para la atribución de la autoría, lo cual ha motivado numerosos estudios y proyectos internacionales. Hay que destacar que si bien se habla de “firma”, ésta no está constituida por trazos manuales del autor, sino por claves, que le pertenecen de un modo indudable. El fundamento técnico para que ello sea posible lo da la criptografía, que estudia la ocultación, disimulación o cifrado de la información y los sistemas que lo permiten. A diferencia del significado que tiene en la cultura de la escritura, en este concepto de firma no tienen cabida la manualidad ni los átomos, sino las claves y los bits.

El procedimiento consiste en la transformación de un mensaje, utilizando un sistema de cifrado asimétrico, de manera que la persona que posea el mensaje inicial y la clave pública del firmante puede determinar de forma fiable si dicha transformación se hizo utilizando la clave privada correspondiente a la clave pública del firmante, y si el mensaje ha sido alterado desde el momento en que se hizo la transformación. La criptografía asimétrica utiliza una doble clave, pública y privada: el que envía un mensaje lo encripta con la clave pública y sólo puede ser decodificado con la clave privada. La clave pública es respaldada por una autoridad certificante de su autoría; la clave privada es sólo atribuible al poseedor, y por lo tanto es asimilable a una firma en el sentido de que es un método fiable para atribuir la autoría de un documento.

Si las claves no pueden ser descubiertas por terceros, es un medio seguro. En este sentido la criptografía simétrica utiliza una misma clave para criptografiar y luego desmontar el procedimiento, mientras que la asimétrica o de clave pública emplea dos claves, una pública y otra privada. La segunda es más confiable ya que su violación requiere averiguar las dos claves, lo cual sería difícil, por lo menos con las técnicas actuales.

La Electronic Signature Record Act (Nueva York, 1999) define en general la firma electrónica como un medio electrónico de identificación, que incluye la firma digital, la cual es única para la persona que la usa, susceptible de verificación, sujeta al único control de la persona que la utiliza, está asociada con datos que garantizan su autenticidad y su integridad y es usada por su titular para que tenga la misma fuerza que la firma a mano.

La firma electrónica es un género, caracterizada por el soporte: todo modo de identificación de autoría basado en medios electrónicos es firma electrónica. Luego vienen las especies que en general se caracterizan por agregar elementos de seguridad que la sola firma electrónica no posee. Las legislaciones reconocen el género de firma electrónica y luego eligen una especie dentro de él, que denominan “firma electrónica avanzada”, o “firma digital”, que es la que utiliza un sistema, generalmente criptográfico, que da seguridad. La gran diferencia estriba en que cuando se utilice la firma digital, se aplican presunciones sobre la identidad del firmante y la integridad del documento que suscriba.

La firma digital tiene las funciones de garantizar la autoría, mantener la confidencialidad, posibilitar el control de acceso limitado, mantener la integridad de la información y asegurar la validez probatoria y los plenos efectos de la firma escrita. En general, tiene los mismos efectos que la firma escrita y no se le puede negar validez sobre la sola base de que no está de forma escrita.

Se admite que la firma digital tiene su principal campo de utilidad en las relaciones comerciales y por ello la legislación excluye su aplicación a las disposiciones por causa de muerte; los actos jurídicos del derecho de familia; los actos personalísimos en general; 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 de acuerdo de partes.

Los riesgos de la firma digital se relacionan con la generación de los datos de la firma, los cuales disminuyen a medida que se mejora la calidad de las instituciones que administran las claves; con la difusión de las claves para lo cual se utiliza la participación de terceros de confianza, que emiten certificados que, a la vez que sirven para distribuir la clave pública, permiten esencialmente asociar de forma segura la identidad de una persona concreta a una clave pública determinada; y con la ineficacia de la firma, relacionada con la validez de la misma en función de si fue creada durante

la vigencia de un certificado digital válido o haber sido debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado

La firma digital requiere un marco institucional que produzca confianza.

Puede haber una firma de este tipo mediante un acuerdo celebrado entre dos partes, las cuales se obligan a reconocerla según los criterios que los contratantes fijen. Sin embargo, el costo de negociar estos acuerdos es alto entre partes que no se conocen o que están situadas en lugares lejanos y no tienen referencias. Por ello, para que exista un uso difundido, rápido, se utiliza un tercero que certifica, el certificador licenciado.

Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u organismos públicos que expide certificados o presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por la autoridad de aplicación.

El certificado digital tiene por función básica la de autorizar la comprobación de la identidad del firmante, pero además debe permitir que el titular lo reconozca indubitadamente y conozca su período de vigencia; determinar que no ha sido revocado; reconocer claramente la inclusión de información no verificada; especificar tal información; contemplar la información necesaria para la verificación de la firma; identificar claramente al emisor del certificado digital.

Infraestructura de firma digital en Argentina

El marco normativo de la República Argentina en materia de Firma digital está constituido por la ley 25506 (B.O. 14/12/2001), el Decreto 2628 (B.O. 20/12/2002) que reglamenta a la misma y un conjunto de normas complementarias que fijan o modifican competencias y establecen procedimientos.

La ley 25506, sancionada el 14 de Noviembre del 2001 tiene como objetivo reconocer el uso de la firma electrónica y la firma digital y su eficacia jurídica en las condiciones que establece la presente ley.

Establece que cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital, principio aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia.

Presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma y 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.

La exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente,

También la ley define a los certificados digitales, requisitos de validez, período de vigencia y reconocimiento de los certificados extranjeros. Fija al certificador licenciado, las funciones del mismo, sus obligaciones y el cese en su calidad como tal. Respecto del titular de un certificado digital, establece sus derechos y obligaciones y fija el sistema de auditoría, al mismo tiempo que crea la Comisión Asesora para la Infraestructura de Firma Digital.

Así queda conformada la infraestructura de firma digital por:

- la Autoridad de aplicación que es la Jefatura de Gabinete de Ministros, quién está facultada a establecer las normas y procedimientos técnicos necesarios para la efectiva implementación de la ley (por medio del Decreto 1028/03 la Oficina Nacional de Tecnologías de Información (ONTI) también está facultada para definir las normas y procedimientos reglamentarios del régimen de Firma Digital);
- la Comisión Asesora para la Infraestructura de Firma Digital que funciona en el ámbito de la Subsecretaría de la Gestión Pública, emitiendo recomendaciones sobre aspectos técnicos referidos al funcionamiento de la Infraestructura de Firma Digital;
- el Ente Licenciante, órgano técnico-administrativo encargado de otorgar las licencias a los certificadores y de supervisar su actividad y que funciona en el ámbito de la Oficina Nacional de Tecnologías de Información (ONTI);
- los Certificadores licenciados que son aquellas personas de existencia ideal, registro público de contratos u organismo público que obtengan una licencia emitida por el ente administrador para actuar como proveedores de servicios de certificación en los términos de la ley 25506 y su normativa complementaria;
- las Autoridades de registro, entidades que tienen a su cargo las funciones de validación y otros datos de los suscriptores de certificados, funciones que son delegadas por el certificador licenciado;

- el Sistema de Auditoría, establecido por la autoridad de aplicación, a fin de evaluar la confiabilidad y calidad de los sistemas utilizados por los certificadores licenciados.

Este marco normativo deroga el Decreto 427/98, cuya aplicación era específica para el Sector Público, por cuanto cubre sus objetivos y alcance.

A su vez, el régimen normativo vigente se complementa con el Decreto N° 1028/2003, el Decreto N° 160/2004, la Resolución JGM N° 435/2004, el Decreto N° 152/2003, el Decreto N° 283/2003, el Decreto N° 1023/2001 y la Resolución SFP N° 194/98.

En el caso particular de la Administración Pública Nacional, se encuentra vigente el Decreto N° 283/03, que autoriza con carácter transitorio a la Oficina Nacional de Tecnologías de Información a proveer certificados digitales para su utilización en aquellos circuitos de la Administración Pública Nacional que requieran firma digital, de acuerdo a la política de certificación vigente.

Independientemente del marco normativo general existente para el Sector Público, existen distintos organismos que han establecido procedimientos o aplicaciones específicas para sus operaciones internas, o para las comunicaciones que establecen con sus administrados que habilitan el uso de documentos electrónicos y firmas digitales como la Resolución del Min. Interior N° 618/2004, la Resolución de Secretaría de Hacienda N° 24/04, la Acordada STJ Jujuy N° 70/2002, la Resolución Administrativa STJ Chubut N° 508/02, la Disposición ONTI N° 5/02, la Resolución JGM N° 176/2002 y la Resolución SGP N° 17/2002.

BIBLIOGRAFÍA

- Acordada STJ Jujuy N° 70/2002
- Amato Mangiameli. Diritto e cyberspace. Giappichelli. Torino. 2000
- Anteproyecto de Ley de Firma Digital- Comisión Redactora del Ministerio de Justicia.
- Baescoechea de Gáname, Ketty Ruth- Sársfield Novillo, Mario. Instrumentos Particulares- Documento Electrónico.
- Cifuentes , Santos. Elementos del derecho civil. Parte general. Es Astrea.
- Código Civil de la República Argentina.
- Código de Comercio de República Argentina.
- Curto, Jorge. El Documento Electrónico- Su eficacia probatoria.
- Dava Rodríguez, Manual de Derecho Informático, Madrid 1997
- Decreto N° 283/2003
- Decreto Ley 290/99 –Portugal
- Decreto Ley 375/99 –Portugal
- Decreto N° 1023/2001
- Decreto N° 1028/2003
- Decreto N° 103/2001
- Decreto N° 152/2003
- Decreto N° 160/2004
- Decreto N° 427/98 del Poder Ejecutivo de la República Argentina.
- Decreto N° 677/2001
- Decreto Reglamentario N° 2628/2002
- Del Piero-Molinari. Proyecto de ley de Comercio Electrónico de la República Argentina.
- Devoto Mauricio. Claves para el éxito de una infraestructura de firma digital. 24/2/2000
- Diccionario de la lengua española- Real Academia Española- 21 edición- Tomo I- Madrid- 1992

- Diniz, Davi, Monteiro. Documentos Electrónicos, Asignaturas Digitales. Ed. LTr. San Pablo 1999
- Directiva de la Unión Europea sobre un Sistema Común para Firmas Electrónicas- 24/5/1999
- Disposición ONTI N° 5/02
- Enciclopedia Salvat. Ed. Salvat Editores S.A. Barcelona.
- Frascchetti, Alejandro. La Ley de Firma Digital y las Presunciones de Autoría e Integridad.
- Gaete Gonzalez, Eugenio Alberto. Documento Electrónico e Instrumento Público.
- Greco, Marco Aurelio. Internet e direito. Ed. Dialéctica. San Pablo. 2000
- Huayamave Betancourt, Xavier. La economía digital. 2000
- Legal Value of Computer Records- Documento de la O.N.U
- Leiva, Juan. Documento Electrónico. Septiembre 2001
- Ley 126-02 de Comercio Electrónico, documentos y firma digital. República Dominicana.
- Ley 19550 de Sociedades Comerciales
- Ley 19799 de Documentos y Firma Digital -12 de Abril de 2002- Chile
- Ley 25506 de Firma Digital- 14 de Noviembre de 2001
- Ley 27269 -Perú
- Ley 527/1999 -Colombia
- Ley 80/525 -12 de Julio de 1980- Legislación francesa.
- Ley de Firma Digital del Estado de Utah -27/2/1995
- Ley Federal del 13/6/1997 -Alemania
- Ley Modelo sobre Comercio Electrónico- Comisión de las Naciones Unidas (UNCITRAL)
- Lorenzetti, Ricardo. Comercio Electrónico. Ed. Abeledo Perrot
- Martínez Nadal. La ley de firma electrónica. Madrid 2000
- Normativa de Firma Digital- 1996- Comité de Seguridad de la Información de la Sección de Ciencia y Tecnología de la American Bar .
- Nuevo diccionario enciclopédico ilustrado. Ed. Sopena Argentina S.A.
- Página web www.angelfire.com.ar
- Página Web www.ca.sgp.gov.ar

- Página Web www.carsoft.com.ar
- Página Web www.definiciones.com.org
- Página web www.mbejane.com.ar
- Página web www.microsiervos.com.ar
- Página Web www.microsoft.com
- Página Web www.monografias.com
- Página Web www.scba.gov.ar
- Página web www.vcd.cl
- Página Web: www.pki.gov.ar
- Pautas de Políticas Criptográficas- Organización de Cooperación y Desarrollo Económico (OCDE)
- Primera conferencia francesa de la organización Xplor International.
- Proyecto de reforma del Código Civil Argentino- 1998
- Real Decreto Ley 14/1999- España
- Resolución Administrativa STJ Chubut N° 508/02
- Resolución del Min. Interior N° 618/2004
- Resolución General N° 345/99
- Resolución JGM N° 176/2002
- Resolución JGM N° 435/2004
- Resolución MTSS N° 555/97- Ministerio de Trabajo y la Seguridad Social
- Resolución SAFJP N° 293/97- Superintendencia de Fondos de Administradores y Pensiones
- Resolución Secretaría de Hacienda N° 24/04
- Resolución SFP N° 194/98
- Resolución SFP N° 194/98- Secretaría de la Función Pública
- Resolución SFP N° 212/97 Secretaría de la Función Pública
- Resolución SFP N° 45/97- Secretaría de la Función Pública
- Resolución SGP N° 17/2002
- Resolución SAFJP N° 293/97
- Rolero, Graciela Lilián. Documento electrónico y firma digital. Necesidad de una legislación específica. II Congreso Internacional de Derechos y Garantías en el siglo XXI. Universidad de Bs. As. Abril 2001.



ÍNDICE GENERAL

<u>INTRODUCCIÓN</u>	3
 <u>CAPÍTULO I</u>	
Cambio Social.....	6
Cambio Tecnológico.....	7
Redes informáticas.....	9
Internet.....	11
La influencia de Internet.....	15
 <u>CAPÍTULO II</u>	
Economía Digital.....	18
 <u>CAPÍTULO III</u>	
Documento electrónico.....	27
Reglas de autoría histórica.....	27
Documento y documentación.....	28
Documento y firma.....	30
Concepto de documentos electrónicos.....	32
Clasificación del documento electrónico.....	34
Documento electrónico original, duplicado y falsificado.....	37
Campo de aplicación.....	37
Conservación.....	38

Valor probatorio de los documentos electrónicos.....	39
Documento electrónico como cosa.....	40
Situación en Argentina.....	41
El documento electrónico en otros países.....	43

CAPÍTULO IV

La firma y la nueva tecnología.....	47
Noción de firma.....	48
La técnica criptográfica.....	48
Definiciones legales y proyectos de ley.....	50
Firma electrónica y firma digital.....	53
Elementos que caracterizan a la firma digital.....	55
Funciones.....	56
Efectos.....	57
Campo de aplicación.....	58
Riesgos de la firma digital.....	59
Certificación.....	61
Autoridades certificadoras.....	61
Eficacia del certificado.....	62
Obligaciones del certificador.....	63
Derechos de los titulares y usuarios de firmas electrónicas.....	64
Responsabilidad de la autoridad certificante.....	65

El lenguaje técnico.....	66
--------------------------	----

CAPÍTULO V

La firma digital en la República Argentina.....	71
---	----

Anteproyecto de ley de firma digital.....	71
---	----

Ley 25506 de Firma Digital.....	79
---------------------------------	----

Infraestructura de firma digital.....	90
---------------------------------------	----

Régimen normativo vigente en la República Argentina.....	91
--	----

Normativa sobre firma digital específica para el Sector Público....	93
---	----

Normativa sobre aplicaciones del sector público.....	93
--	----

Subsecretaría de la Gestión Pública.....	96
--	----

<u>CONCLUSIÓN</u>	100
-------------------------	-----

<u>RESUMEN DEL TRABAJO FINAL</u>	103
--	-----

<u>BIBLIOGRAFÍA</u>	112
---------------------------	-----

U.N.R.C.
Biblioteca Central



61150

61150