Legislación Aplicable a la Tecnología y a las Comunicaciones

Alumno: Ariel Mendez

**Documento Electrónico**

¿Qué es un Documento Electrónico?

Documento Electrónico es el documento gestado con intervención de un

ordenador, que hacen perceptibles y comprensibles las señales digitales

(magnéticas) de que están constituidos, los datos están en el mismo

ordenador; que no es comprensible para el operador.

Esta formado por un grupo de bits (números binarios: ceros y unos) que en su

conjunto representan los caracteres que integran el documento y que podría

encontrarse físicamente alojado en un soporte magnético (discos rígidos,

unidades de disquetes, cintas de almacenamiento, zips, cdrom, etc.) pudiendo

ser visualizado o impreso.

Tenemos entonces el Documento creado por la computadora (Doc.

Constituyente) y el creado por medio de la computadora (Doc. Comprueba)

Según su permanencia en el tiempo, puede clasificar:

* Volátil, se pierde con el corte de energía (memoria)
* Inalterables, son aquellos que una vez guardados no pueden

alterarse, solo leídos (CD-ROM)

La definición que creemos que es más clara y correcta es la de Chile, cuando

expresa en su “Ley de Doc. Electrónico y Firma Electrónica” lo siguiente:

Documento Electrónico: 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.

¿Qué diferencia un documento en papel de un documento electrónico?

Lo que marca su diferencia es el soporte que contiene la información. Estos

documentos continúan siendo los mismos y responden a los mismos

planteamientos de creación, lo que se incorpora ahora son nuevos soportes

que contienen información.

Los documentos electrónicos generados en el ámbito de gestión y

administración de una organización pública resulta ser tan probatorio de

derechos y obligaciones de partes como los documentos generados en soporte

papel, pergamino o papiro.

El documento electrónico, tiene datos o informaciones que tienen relevancia

jurídica los cuales son transmitidos por vía electrónica especialmente a través

del procesamiento electrónico de datos o simples soportes de sonido. La

problemática central en la contratación electrónica gira alrededor de la validez

jurídica del soporte de la documentación en medios informáticos, es decir, la

validez del denominado documento electrónico.

**Firma Digital**

¿Qué es la Firma Digital?

La firma digital es una herramienta tecnológica que permite comprobar quién

es el autor de un documento y verificar que su contenido no haya sido

modificado. Por ello, un documento electrónico firmado digitalmente posee la

misma validez jurídica que un documento en papel firmado de puño y letra, en

tanto y en cuanto exista la normativa que le dé pleno valor legal a la misma.

Podemos decir que la firma digital es el conjunto de caracteres que se añaden

al final de un documento o cuerpo de un mensaje para informar, dar fe o

mostrar validez y seguridad. La firma digital sirve para identificar a la persona

emisora de dicho mensaje y para certificar la veracidad de que el documento

no se ha modificado con respeto al original. No se puede negar haberlo

firmado, puesto que esta firma implica la existencia de un certificado oficial

emitido por un organismo o institución que valida la firma y la identidad de la

persona que la realiza.

En la elaboración de una firma digital se utiliza una técnica de criptografía

asimétrica. Esto es, que para firmar documentos electrónicamente, cada

persona necesita un par de claves criptográficas:

• Una clave privada que está bajo absoluto control del suscriptor y

solo este conoce, que la almacena de forma segura en su

computadora, celular o dispositivo criptográfico. Esta clave le servirá

para firmar los documentos, mediante un proceso criptográfico que

tiene como entrada esta clave, más el documento que se desea

firmar; y como salida, el documento firmado electrónicamente.

• Una clave pública, matemáticamente asociada a la privada, que

puede compartirse con todo el mundo. Mediante otro proceso

criptográfico, puede comprobarse con esta clave que un documento

fue firmado electrónicamente utilizando la clave privad

correspondiente (lo que asegura el no repudio, ya que esa clave

privada solo la conoce el emisor y entonces nadie más puede

utilizarla para firmar el documento) y que no fue alterado

(asegurando así la integridad).

Firma Digital y el Sector Público

En la Republica Argentina la Resolución 45/1997 de la secretaria de la Función

Pública, autorizo el empleo de la firma digital en todo el ámbito del sector

Publico , y el decreto 427/1998 del 16/04/1998 estableció concretamente el

empleo de la firma digital en la instrumentación de los actos internos, que no

produzcan efectos jurídicos individuales en forma directa, disponiendo la

creación de Infraestructura de Firma Digital para la Administración Pública

Nacional (FDAPN) y Autorizando el empleo de la firma digital por un plazo de

dos años , a contar del dictado de los manuales de procedimientos y de los

estándares tecnológicos.

**Firma Electrónica**

¿Qué es la Firma Electrónica?

Si bien por firma electrónica se puede entender cualquier sistema utilizado en

medios de comunicación electrónica como símbolo de identificación personal,

Jurídicamente hablando la firma electrónica es descripta como el conjunto de

datos Electrónicos integrados, ligados y asociados de manera lógica a otros

datos electrónicos, utilizado por el signatario como su medio de identificación,

que carezca de alguno de los requisitos legales para ser considerada firma

digital.

Para firmar un documento hay varias técnicas a emplear para la Firma

Electrónica, ejemplo:

* Código secreto o de ingreso, combinación de letras y/o números

conocida por el dueño del documento.

* Métodos basados en la Biométrica, se accede al documento

mediante mecanismos de identificación física o biológica del

usuario o dueño del documento. Consiste en la comparación de

características físicas de cada persona con un patrón conocido

y almacenado en una base de datos. Los lectores biométricos

identifican a la persona por lo que es (manos, ojos, huellas

digitales y voz).

* Criptografía (cifrado de mensajes): Esta consiste en un sistema

de codificación de un texto con claves de carácter confidencial y

procesos matemáticos complejos, de manera que para el

tercero resulta incomprensible el documento si desconoce la

clave decodificadora, que permite ver el documento en su forma

original.

**¿Firma Digital y Firma Electrónica son lo mismo?**

Para poder responder esta cuestión, necesitamos tener en cuenta para qué

firmamos documentos, qué busca manifestar el ente/el usuario con ello:

• Autoría: Es decir, determinar con certeza el autor de un documento, la

firma va acompañada generalmente de una aclaración con el nombre y

apellido de la persona que firma.

• Integridad: Una vez firmado un documento, este no puede ser alterado

mediante nuevas anotaciones, tachaduras, etc. En soporte papel, cuando

esto sucede, las mismas deben ser observadas.

• No repudio: El autor no puede negar su autoría o decir que no es lo que

firmó originalmente, ya que su firma es única y puede comprobarse que

efectivamente la realizó mediante pericias caligráficas. El no repudio es un

atributo que lo establece la jurisprudencia de cada país que incorpora esta

tecnología.

Legalmente, la diferencia radica en el valor probatorio atribuido a cada una de

ellas ya que la ley establece una presunción “iuris tantum” de autoría e

integridad respecto a la firma digital, la reconoce como procedimiento técnico,

seguro y confiable.

**Delitos informáticos**

**¿Qué es un delito informático?**

Un delito informático es un acto dirigido contra la confidencialidad, la integridad y la

disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de

dichos sistemas, redes y datos.

Otra definición adicionando la anterior es que el delito informático implica cualquier actividad

ilegal que encuadra en figuras tradicionales ya conocidas como robo, hurto, fraude,

falsificación, perjuicio, estafa y sabotaje, pero siempre que involucre la informática de por

medio para cometer la ilegalidad.

Las categorías que definen un delito informático son aún mayores y complejas y pueden

incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de

caudales públicos en los cuales ordenadores y redes han sido utilizados. Con el desarrollo de

la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y

sofisticados.

Fraude puede ser definido como engaño, acción contraria a la verdad o a la rectitud. La

definición de Delito puede ser más compleja.

Muchos derechos de Derecho Penal han intentado formular una noción de delito que sirviese

para todos los tiempos y en todos los países. Esto no ha sido posible dada la íntima conexión

que existe entre la vida social y la jurídica de cada pueblo y cada siglo, aquella condiciona a

esta.

Se podría definir el delito informático como toda acción (acción u omisión) culpable realizada

por un ser humano, que cause un perjuicio a personas que necesariamente se beneficie el

autor o que, por el contrario, produzca un beneficio ilícito a su autor, aunque no perjudique

de forma directa o indirecta a la víctima, tipificando por la ley que se realiza en el entorno

informático y está sancionado con una pena.

Contemplando el delito informático en un sentido amplio se puede formar varios grandes

grupos de figuras delictivas claramente diferenciadas:

* Delitos contra la intimidad
* Delitos contra el patrimonio
* Falsedades documentales

La Organización de Naciones Unidas reconoce los siguientes tipos de delitos informáticos:

* Fraudes cometidos mediante manipulación de computadoras; en este se reúne: la

manipulación de datos de entrada (sustraer datos), manipulación de programas

(modificar programas del sistema o insertar nuevos programas o rutinas),

manipulación de los datos de salida (fijación de un objeto al funcionamiento de

sistemas de información, el caso de los cajeros automáticos) y fraude efectuado por

manipulación informática (se sacan pequeñas cantidades de dinero de unas cuentas a

otras).

* Manipulación de datos de entrada; como objetivo cuando se altera directamente los

datos de una información computarizada. Como instrumento cuando se usan las

computadoras como medio de falsificación de documentos.

* Daños o modificaciones de programas o datos computarizados; entran tres formas de

delitos: sabotaje informático (eliminar o modificar sin autorización funciones o datos

de una computadora con el objeto de obstaculizar el funcionamiento) y acceso no

autorizado a servicios y sistemas informáticos (ya sea por curiosidad, espionaje o por

sabotaje).

Características de los delitos informáticos

* Son conductas criminógenas de cuello blanco (White collar crimes), en tanto que sólo

determinado número de personas con ciertos conocimientos (en este caso técnicos)

pueden llegar a cometerlas.

* Son acciones ocupacionales, en cuanto que muchas veces se realizan cuando el sujeto

se halla trabajando.

* Son acciones de oportunidad, en cuanto que se aprovecha una ocasión creada o

altamente intensificada en el mundo de funciones y organizaciones del sistema

tecnológico y económico.

* Provocan serias pérdidas económicas, ya que casi siempre producen beneficios de

más de cinco cifras a aquellos que los realizan.

* Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una

necesaria presencia física pueden llegar a consumarse.

**Delitos en Perspectiva**

Los delitos pueden ser examinados desde dos puntos de vista diferentes:

* Los delitos que causan mayor impacto a las organizaciones.
* Los delitos más difíciles de detectar.

Aunque depende en gran medida del tipo de organización, se puede mencionar que los

Fraudes y sabotajes son los delitos de mayor incidencia en las organizaciones. Además,

aquellos que no están claramente definidos y publicados dentro de la organización como un

delito (piratería, mala utilización de la información, omisión deliberada de controles, uso no

autorizado de activos y/o servicios computacionales; y que en algún momento pueden

generar un impacto a largo plazo).

Pero si se examina la otra perspectiva, referente a los delitos de difícil detección, se deben

situar a aquellos producidos por las personas que trabajan internamente en una organización

y que conocen perfectamente la configuración interna de las plataformas; especialmente

cuando existe una cooperación entre empleados, cooperación entre empleados y terceros, o

incluso el involucramiento de la administración misma.

Sujeto Activo

Los Elementos del delito necesarios para estudiar este tipo de conductas son:

* Sujeto: Autor de la conducta ilícita o delictiva
* Medio: El sistema informático
* Objeto: El bien que produce el beneficio económico o ilícito

Los sujetos involucrados en la comisión de delitos informáticos son: sujeto activo y sujeto

pasivo. Los sujetos activos, son personas de cierto estatus socioeconómico, es decir, son

personas que poseen ciertas características que no presentan el común de los delincuentes,

esto es, los sujetos activos, tienen habilidades para el manejo de los sistemas informáticos y

electrónicos.

**Sujeto Pasivo**

En primer término, es necesario recordar que el sujeto pasivo del delito, es la persona física o

moral que resiente la actividad delictiva, es el titular del bien jurídicamente tutelado que es

dañado o puesto en peligro por la conducta del agente, y en los casos de los delitos

informáticos pueden ser individuos particulares, personas morales como sociedades

mercantiles, instituciones crediticias, gobiernos etcétera, que usan sistemas automatizados de

información, generalmente conectados a otros.

El sujeto pasivo que me ocupa y preocupa, es sumamente importante para el estudio de los

delitos objeto de este estudio, ya que, mediante él, es posible conocer los diferentes ilícitos

que cometen los activos informáticos, con objeto de prever las acciones antes mencionadas

debido a que muchos de los delitos son descubiertos por casualidad, desconociendo el Modus

operandi de los agentes delictivos.

**Clasificación de los delitos informáticos**

Los delitos informáticos se clasifican en base a dos criterios:

como instrumento o medio, o como fin u objetivo.

Como medio y objetivo:

en esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la

computadora, accesorios o programas como entidad física. Se presenta una clasificación, de lo

que ella llama delitos electrónicos, diciendo que existen tres categorías:

Los que utilizan la tecnología electrónica como método;

Los que utilizan la tecnología electrónica como medio; y

Los que utilizan la tecnología electrónica como fin.

Como método: conductas criminales en donde los individuos utilizan métodos electrónicos

para llegar a un resultado ilícito.

Como objeto: Es cuando se alteran datos de documentos que se encuentran almacenados en

forma computarizada. Pueden falsificarse o adulterarse también micro formas, micro

duplicados y microcopias; esto puede llevarse a cabo en el proceso de copiado o en cualquier

otro momento.

Como instrumentos o medio

Como instrumento: Las computadoras pueden utilizarse para realizar falsificaciones de

documentos de uso comercial. Las fotocopiadoras computarizadas en colora base de rayos

láser dieron lugar a nuevas falsificaciones. Estas fotocopiadoras pueden hacer copias de alta

resolución, modificar documentos, crear documentos falsos sin tener que recurrir a un

original, y los documentos que producen son de tal calidad que solo un experto puede

diferenciarlos delos documentos auténticos.

Como medio: son conductas criminógenas en donde para realizar un delito utilizan una

computadora como medio o símbolo.

En esta categoría se encuentran las conductas criminales que se valen de las computadoras

como método, medio o símbolo en la comisión del ilícito, por ejemplo:

1. Falsificación de documentos vía computarizada (tarjetas de crédito, cheques.)

2. Variación de los activos y pasivos en la situación contable de las empresas.

3. Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude.)

4. Lectura, sustracción o copiado de información confidencial.

5. Modificación de datos tanto en la entrada como en la salida.

6. Aprovechamiento indebido o violación de un código para penetrar a un sistema

introduciendo instrucciones inapropiadas.

7. Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta

bancaria apócrifa.

**Como fin u objetivo**

Como fin: conductas criminógenas dirigidas contra la entidad física del objeto o máquina

electrónica o su material con objeto de dañarla.

Como fin u objetivo: En esta categoría, se enmarcan las conductas criminales que van

dirigidas contra las computadoras, accesorios o programas como entidad física, como, por

ejemplo:

1. Programación de instrucciones que producen un bloqueo total al sistema.

2. Destrucción de programas por cualquier método.

3. Daño a la memoria.

4. Atentado físico contra la máquina o sus accesorios.

5. Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los

centros neurálgicos computarizados.

6. Secuestro de soportes magnéticos entre los que figure información valiosa con fines

de chantaje.

Crímenes específicos

Sabotaje informático

Implica que el delincuente recupere o busca destruir el centro de cómputos en sí (las

máquinas) o los programas o informaciones almacenados en los ordenadores. Se presenta

como uno de los comportamientos más frecuentes y de mayor gravedad en el ámbito político.

Piratería informática

La piratería informática consiste en la violación ilegal del derecho de autor. Según la definición

que en su artículo 51 brinda el ADPIC (Acuerdo sobre los aspectos de los Derechos de

propiedad Intelectual) son aquellas mercaderías que lesionan el derecho de autor. La

piratería es una de las modalidades de reproducción técnica (la otra es la -reproducción burda

del original cuya apariencia dista mucho de la auténtica), que implica la elaboración de una

copia semejante al original, con la intención de hacerla pasar por tal.

Existen dos modalidades que se incluyen como piratería informática a saber:

1. El hurto de tiempo de máquina: consiste en el empleo del computador sin

autorización, y se pretende aludir a situaciones en que un tercero utiliza

indebidamente recursos de la empresa en que trabaja o un sujeto autorizados se vale

de tales prestaciones informáticas en un horario no permitido, utilizándolas para su

provecho sin contar con permiso para ese uso fuera de hora.

2. La apropiación o hurto de software y datos: en este caso el sujeto accede a un

computador ajeno o a la sesión de otro usuario, retirando archivos informáticos,

mediante la ejecución de los comandos copiar o cortar, para luego guardar ese

contenido en un soporte propio.

Cajeros automáticos y tarjetas de crédito

Conductas mediante las cuales se logra retirar dinero del cajero automático, utilizando una

tarjeta magnética robada, o los números de la clave para el acceso a la cuenta con fondos.

El caso Chalmskinn

Se procede cuando se accede a ordenadores industriales centrales de la red para el uso

específico de malgastar fondos para interrumpir los accesos a telefonía móvil, más conocido

como el caso Chalmskinn.

Robo de identidad

Luego de obtener los datos personales de un individuo, se procede a realizar todo tipo de

operaciones para provecho del victimario, fingiendo ser la persona a la que se extrajo su

información sensible. Encuadra como delito de estafa. Si el actuar del sujeto activo comporta

dar a conocer datos personales ajenos contenidos en base de datos a las que por su empleo

tiene acceso, entonces por expreso mandato legal la figura aplicable es la de revelación de

secreto profesional.

Phreaking

Es la metodología más antigua dentro de los denominados ciberdelitos, consiste en ingresar

en las redes de telecomunicaciones para realizar llamadas telefónicas a larga distancia

utilizando la cuenta ajena. Resulta ser una modalidad primitiva de hacking.

**Comercio Electrónico**

El comercio electrónico era cualquier forma de transacción de negocios en las cuales las partes

interactúan electrónicamente en lugar de hacerlo de forma física. Pero con la llegada de Internet, a mediados de los 90’ se

refiere a la venta de bienes y servicios a través de internet, utilizando como forma de pago medios electrónicos.

Se puede afirmar que se trata del intercambio de bienes y/o servicios utilizando medios electrónicos en por lo

menos alguna etapa de una transacción comercial.

La diferencia fundamental con las formas de comercio tradicional y la necesidad de replanteos jurídicos surgen a

partir del cambio en la instrumentación de los negocios. Con la utilización de las nuevas tecnologías en las relaciones

comerciales, se abandona el soporte de los mensajes sobre papel y se lo reemplaza por soportes magnéticos o

electrónicos

Sin dudas el comercio electrónico es un reflejo del proceso de globalización mundial de la economía donde el

espacio y el tiempo se desnaturalizan. Pero si bien las tecnologías evolucionan rápidamente, las costumbres son más

reticentes a los cambios, siendo la inseguridad e incertidumbre en la utilización de los medios electrónicos una de las

principales barreras locales al crecimiento del comercio electrónico.

**Tipos De Comercio Electrónico**

Existen dos clases de comercio electrónico:

Indirecto: Consiste básicamente en adquirir productos o bienes tangibles que necesitan luego ser enviados

físicamente al comprador utilizando medios de distribución convencionales como envío postal, encomiendas, etc.

Directo: Es aquel mediante el cual el pedido, el pago y el envío de los bienes intangibles y/o servicios se producen

“on-line” (programas informáticos, servicios de información). Permite transacciones electrónicas de extremo a extremo sin

obstáculos a través de las fronteras geográficas, aprovechando todo el potencial de los mercados electrónicos

mundiales.

**¿Para qué sirve el comercio electrónico?**

sobre 3 cosas para las que sirve el e-commerce.

### 1. Incremento de las oportunidades de venta

Lógicamente, un comercio que opere de forma tradicional incrementará de forma significativa sus oportunidades de venta si también decide aprovechar los canales electrónicos.

Por otro lado, las [marcas](https://rockcontent.com/es/blog/como-crear-una-marca/) que se dedican exclusivamente a esta forma de comercio también cuentan con mayores oportunidades, pues tienen acceso a una comunidad global de millones de usuarios.

### 2. Lanzamiento de productos innovadores

En el mercado tradicional, el lanzamiento de [productos innovadores](https://rockcontent.com/es/blog/innovacion-disruptiva/) demanda una fuerte inversión en [publicidad](https://rockcontent.com/es/blog/publicidad/) y una gran estructura logística para llevarlo a los puntos de venta o proveedores adecuados, así como la productividad de un equipo de venta.

Es por eso que muchos medianos y pequeños emprendedores aprovechan el comercio electrónico para ofrecer servicios o artículos novedosos, permitiéndoles a los usuarios conocer sus especificaciones e, incluso, interactuar con algunas de sus funcionalidades antes de comprarlos.

### 3. Reconocimiento de marca

Si tu negocio tiene años de trayectoria, pero su reconocimiento de marca es muy bajo, sin duda necesitas del comercio electrónico.

Comercializar en la numerosa comunidad de Internet y las redes sociales sirve para que una marca pase de ser “invisible” a conocida por muchos usuarios y actores del mercado.

**Regulación del comercio electrónico**

**Principales Modelos Internacionales**

Múltiples son los modelos internacionales relacionados con el comercio electrónico, en base a los cuales se han

estructurado los regímenes legales de Comercio Electrónico de los estados. De entre ellos hemos elegido tres, por

considerarlos importantes, de los cuales haremos un breve comentario.

• La Ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil

Internacional. CNUDM.

• La Directiva de la Unión Europea sobre Comercio Electronic, Directiva 2000/31/CE del Parlamento Europeo y del

Consejo de 8 de junio de 2000 y la Directiva de la Unión Europea sobre los derechos de los consumidores, directiva

2011/83/UE del Parlamento Europeo y del Consejo del 25 de octubre de 2011.

**Principales disposiciones de los modelos**

**Modelo de la Comisión de Naciones Unidas para el Derecho Mercantil Internacional CNUDMI**

Durante las últimas décadas la Organización de la Naciones Unidas a través de su Comisión para el Derecho Mercantil

Internacional (CNUDMI) , ha venido cumpliendo una invalorable labor en miras a una unificación legislativa del derecho

mercantil internacional elaborando numerosos convenios y recomendaciones. [2]

En este marco se confeccionó la Ley Modelo de la CNUDMI sobre Comercio Electrónico y otros medios conexos de

comunicación de datos, que fue aprobada en Nueva York en 1996, y cuya principal finalidad fue tratar de fomentar la

armonización y unificación del derecho mercantil electrónico internacional.

A partir de entonces se formularon diversas recomendaciones los estados, destacándose entre ellas la aprobada por la

Asamblea General en su resolución 40/1971, inciso b) del párrafo 5, del 11 diciembre de 1985, denominada

"Recomendación de la CNUDMI 1985", en donde se efectúa una serie de recomendaciones y se pide los gobiernos y a las

organizaciones internacionales que, cuando a convenir, adopten medidas de conformidad con la recomendación de la

Comisión a fin de garantizar la seguridad jurídica en el contexto de la utilización más amplia posible del procesamiento

automático de datos en el comercio internacional.

La finalidad de la Ley Modelo es la de ofrecer al legislador nacional un conjunto de reglas aceptables en el ámbito

internacional que le permitan eliminar algunos de esos obstáculos jurídicos con miras a crear un marco jurídico que

permita un desarrollo más seguro de las vías electrónicas de negociación designadas por el nombre de "comercio

electrónico".

Conforme a su artículo primero la ley será aplicable "a todo tipo de información en forma de mensaje de datos utilizada

en el contexto de actividades comerciales".

La ley recomienda así que los estados que adopten el modelo traten de regular las distintas tecnologías pero

manteniendo la flexibilidad del sistema, resaltando que se ha adoptado en el modelo el criterio del equivalente funcional

entre los conceptos tradicionales de firma, escritura y original, y el alcance moderno que debe darse a esos términos. Este

criterio del equivalente funcional fue desarrollado años después por la Ley Modelo de la CNUDMI de Firmas Electrónicas

del año 2001.

**La Directiva de la Unión Europea**

La primera de ellas, que llamaremos Directiva sobre Comercio Electrónico, se basa en las orientaciones de la Iniciativa Europea de Comercio Electrónico de 1997, relativa al comercio electrónico, cuyo objetivo era la creación de un marco jurídico coherente a escala europea en este sector. La estrategia consiste, en particular, en evitar un exceso de reglamentación, y para ello se inspira en las libertades del mercado interior, teniendo en cuenta las realidades comerciales, y se propone dar una protección eficaz a los objetivos de interés general. Se aplica, fundamentalmente, en los sectores y actividades siguientes: periódicos en línea, bases de datos en línea, servicios financieros en línea, servicios profesionales en línea (abogados, médicos, contables, agentes inmobiliarios), servicios recreativos en línea (p.ej., alquiler de vídeos), marketing y publicidad directas en línea y servicios de acceso a

Internet.

● La Directiva se aplica especialmente a los prestadores de servicios establecidos en la Unión Europea (UE). Sin embargo,

para no obstaculizar el comercio electrónico mundial, se propone también evitar incompatibilidades con la evolución

jurídica de otras regiones del mundo.

● La Directiva prohíbe que los Estados miembros impongan a los servicios de la sociedad de la información regímenes de autorización especiales que no se aplicarían a otros servicios similares prestados por otros medios.

● Los Estados miembros deben establecer en su legislación que los prestadores de servicios de la sociedad de la información puedan facilitar a los destinatarios de los servicios y a las autoridades competentes un acceso fácil, directo y permanente a la información relativa a sus actividades: nombre, dirección, dirección electrónica, número de inscripción en el registro mercantil, título profesional, afiliación a organizaciones profesionales, número de IVA.

● La Directiva se aplica especialmente a los prestadores de servicios establecidos en la Unión Europea (UE). Sin embargo,

para no obstaculizar el comercio electrónico mundial, se propone también evitar incompatibilidades con la evolución

jurídica de otras regiones del mundo.

● La Directiva prohíbe que los Estados miembros impongan a los servicios de la sociedad de la información regímenes de

autorización especiales que no se aplicarían a otros servicios similares prestados por otros medios.

● Los Estados miembros deben establecer en su legislación que los prestadores de servicios de la sociedad de la

información puedan facilitar a los destinatarios de los servicios y a las autoridades competentes un acceso fácil, directo y

permanente a la información relativa a sus actividades: nombre, dirección, dirección electrónica, número de inscripción

en el registro mercantil, título profesional, afiliación a organizaciones profesionales, número de IVA.

**La contratación electrónica**

Particularidades y cuestiones a resolver.

El comercio electrónico realizado a través de Internet conlleva implícita la celebración de diferentes contratos mercantiles propios de la forma operacional del negocio. La mayoría de los contratos se celebran utilizando medioselectrónicos en por lo menos alguna de sus etapas de formación o ejecución. Así, si se analiza la operatoria contractual del comercio electrónico en su versión “BtoC” (business to consumer, o sea, del comerciante al consumidor) encontramos en la relación comerciante/consumidor la concreción de contratos de compraventa de bienes muebles o de locación de servicios, entre otros. Asimismo, y posibilitando la estructura y funcionamiento del sitio en la web, la empresa que lleva adelante el negocio virtual celebra con agentes externos, tales como las telefónicas, los ISP (Internet Services Providers, o proveedores de servicios de Internet), los transportistas, los seguros, los diseñadores, los técnicos, el sector publicitario, las licencias de marcas y tecnologías, los proveedores, el registro de nombres de dominio, distintos contratos de compraventa, locación de obra y de servicios, de seguros, de licenciamiento, etc. El contrato no deja de ser el resultado de la concurrencia de voluntades con distintos intereses, el cambio radical se evidencia en la instrumentación de tales acuerdos, al abandonarse el soporte de las ideas sobre papel para utilizar soportes electrónicos. En principio, y por lo que antecede, la tradicional teoría de los contratos resulta aplicable a esta nueva modalidad de contratación. Las cuestiones novedosas y principales que demandan atención y solución jurídica se

refieren a:

1) la validez y fuerza probatoria del documento electrónico,

2) la identificación de las partes que interactúan, y

3) al no repudio del contenido de las manifestaciones de voluntad realizadas.

Hasta el momento los sistemas que pueden garantizar un principio de solución para las exigencias de confiabilidad, integridad, transmisión y conservación que debe respetar todo documento electrónico son la encriptación de la información y la certificación electrónica, ambas en el marco de aplicación de una infraestructura de firma digital.

**Contratos electrónicos de consumo**

La Ley de Defensa del Consumidor (Ley No 24.240) vigente en la Argentina desde el año 1993 incluye entre sus normas específicamente algunos aspectos de la venta por medios electrónicos o similares. En tal supuesto, se reconoce al consumidor la facultad irrenunciable de revocar la aceptación de la oferta dentro de los cinco días posteriores a la entrega de la cosa o celebración del contrato, según corresponda, sin responsabilidad ni cargo alguno. Asimismo, y atinente al tema en estudio se destaca que la Ley de Defensa del Consumidor introdujo significativos cambios con relación a la obligatoriedad de la oferta disponiendo la validez de la oferta dirigida a consumidores potenciales indeterminados y obligando a quien la emite durante el tiempo en que se realice.

**Dominio y Marca**

**Dominio**

El dominio es el nombre que identifica a un sitio determinado en internet

(similar a una dirección física), están relacionados por un número de IP.

El dominio www.dominio.com.ar, por ejemplo, tiene varios componentes. El

primero se refiere a la " World Wide Web" (Gran Red Mundial). El segundo es parte

del dominio que identifica al sitio en cuestión. El tercero ".com" es la extensión que

identifica la actividad de la organización (.com, comercial; .org, organización no

lucrativa; .edu, organización educativa; .gov, organización gubernamental).

Su registro difiere del ente del cual los registra, el caso más común si el

dominio es “.com” son gestionados por la ICANN.

Por otra parte los “.com.ar” es de Argentina y los gestiona NICAR que

depende del ministerio de relaciones exteriores.

El registro de un determinado “dominio” es otorgado al primero que lo solicite.

El formulario el cual llena al momento de registrar el dominio tiene carácter de

declaración jurada.

El hecho que NIC Argentina registre un nombre de dominio a favor de un

registrante, no implica que asuma responsabilidad alguna respecto de la legalidad de

ese registro ni del uso del nombre de dominio por el registrante.

El periodo de duración de un dominio corresponde a 1 año a partir de la

fecha de inscripción, siendo posible la renovación.

**Marcas**

Una marca es un signo con capacidad distintiva que permite diferenciar de

los demás aquellos productos o servicios que son propiedad de una persona o

empresa. Registrarla te otorga el título de propiedad y derecho exclusivo sobre ella.

Existen 45 tipos de clases en la que se puede registrar una marca. Esto

depende en sí del producto o servicio en particular que se vaya a identificar. Por

ejemplo, un Hotel registrar el nombre bajo la clase 43: “SERVICIOS DE

RESTAURACIÓN (ALIMENTACIÓN); HOSPEDAJE TEMPORAL”. En cambio, si se

registra un par de zapatos, clasifica bajo la clase 25: “VESTIDOS, CALZADOS,

SOMBRERERÍA”. Las 45 clases se pueden encontrar en [www.inpi.gob.ar](http://www.inpi.gob.ar).

Existen diferentes tipos de marcas:

● Denominativas: Compuestas única y exclusivamente por palabras,

letras o números y sus combinaciones, sin reivindicar características

gráficas o color específico.

● Figurativas: Símbolos gráficos, dibujos e isotipos.

● Mixtas: Se integran por la combinación de elementos denominativos y

figurativos a la vez, o de elementos nominativos cuya grafía se presente

de forma estilizada.

**Registro de la marca**

El primer paso es buscar si la marca se encuentra disponible. Para ello

Consultá los distintos tipos de clases de marca antes mencionados a través de su

sitio web, y de esta forma comprobar a qué tipo puede pertenecer una marca según

el nomenclador Internacional establecido por Ley 26230.

Consultar en el buscador del mismo sitio web si la marca se encuentra

disponible. En caso de aparecer la leyenda “no hay resultados que correspondan

con su criterio de búsqueda”, buscar con diferentes variantes (escrita con otras

letras, en singular o plural, etc) para ver que no haya ninguna marca similar. Si no

hay resultados, el trámite se podrá iniciar.

Otra forma de buscar la disponibilidad de la marca es presencialmente en la

Mesa De Informes de la Dirección Nacional de Marcas, en Av. Paseo Colón 717

Planta Baja, Ciudad Autónoma de Buenos Aires, C1063ACH.

Entre otros datos, también debe informarse la titularidad de la marca. Por

ejemplo: cuántos titulares tendrá, que porcentaje le corresponde a cada uno, etc.

Cuando se carga una solicitud a nombre de más de un titular, se deberá adjuntar al

finalizar una nota escaneada con el consentimiento expreso del resto de los titulares

validando el usuario que ingresó con su clave fiscal. En el caso de cargar dos o más

titulares, el total de los porcentajes deberá resultar 100% y se debe completar la

información correspondiente del formulario para cada uno de dichos titulares.

Si corresponde, se establecen las prioridades de la marca. Si una solicitud

tiene un origen en otra primera solicitud efectuada en otro país, se puede invocar la

prioridad ante el INPI.

**Como se inscribe**

● En línea: ingresando al portal de trámites del INPI con una clave

fiscal. El trámite que se ingrese a través del Portal Web en el que se

verifique la utilización de una clave fiscal diferente a la del solicitante,

su apoderado, o su representante legal, deberá ser ratificado dentro

del plazo de cuarenta (40) días hábiles posteriores a su ingreso bajo

apercibimiento de tener por no presentado dicho trámite.

● Personalmente: se deberán descargar los formularios (en versión pdf

o en planilla de cálculo y completarlos. Luego aquellos papeles deben

presentarse en la Mesa General de Entradas del INPI, Av. Paseo

Colón 717 Planta Baja, Ciudad Autónoma de Buenos Aires,

C1063ACH. Abonando el arancel de solicitud de registro (timbrado)

en la tesorería ubicada en la planta baja.

● Por correo postal: se tendrán que descargar los formularios (en

versión pdf o en planilla de cálculo y completarlos. Abonar el arancel

de solicitud de registro por giro postal a nombre de INPI 5100/622

RECAUDADORA FF 12 por los aranceles que correspondan ser

abonados. Remitir por Correo Argentino los formularios,

**Conflicto entre marca y dominio**

Como hemos comentado anteriormente, registrar una marca es un trámite

que lleva una serie de pasos (y que incluso la solicitud de la marca puede ser

rechazada). Mientras que el dominio es un trámite mucho más rápido, casi

instantáneo.

Muchas veces puede ocurrir que una marca quiere registrar su marca en un

dominio web y se encuentre con que esta ya esta siendo usada.

Como hemos comentado anteriormente, registrar una marca es un trámite

que lleva una serie de pasos (y que incluso la solicitud de la marca puede ser

rechazada). Mientras que el dominio es un trámite mucho más rápido, casi

instantáneo.

Muchas veces puede ocurrir que una marca quiere registrar su marca en un

dominio web y se encuentre con que esta ya siendo usada.

**Casos de conflictos**

PSA

Con PSA sucedió el mismo caso que con Freddo, alguien ya tenía la marca

registrada.

El hecho de tener la marca, es excluyente del uso legítimo del titular en el

ámbito de Internet.

El registro del dominio, calificado por la Excma Cámara como uso indebido

de marca, impedía al legítimo titular acceder al mercado de Internet con su propia

marca, constituir su propio sitio y distribuir sus productos desde allí.

Se impuso una multa de 20.000 $

De este caso se puede extraer las siguientes afirmaciones:

● El registro de un dominio idéntico a una marca de propiedad de un tercero

equivale al uso indebido de esa marca.

● El uso indebido es un uso calificado por la especial característica de impedir

al titular del registro marcario el uso de la marca en Internet.

● Carece de trascendencia, al menos no surge de las resoluciones, la buena o

mala fe del registrante del dominio.

● Debido a las características especiales de la infracción marcaria, excluyente

de la posibilidad de uso de la marca en Internet para el titular, la medida

cautelar puede ser un anticipo de la sentencia.

● No se hace mención en las resoluciones al principio de especialidad.

**CASO FREDDO**

Freddo toma la decisión de registrar un dominio en internet para poder

comerciar sus productos. Al intentar hacerlo descubre que el dominio había sido

registrado por otra empresa.

A Través de sus abogados freddo envió varias cartas documento a la

empresa Spot Network intimando a la baja del dominio. Al no recibir respuesta, el 24

Noviembre iniciaron una demanda judicial. La causa es conocida como causa

testigo.

En primera instancia el dominio a freddo fue otorgado hasta sentencia

definitiva. En abril del año 1999 se llegó a un acuerdo por el cual la empresa

denunciada se comprometió a no usar mas el nombre de freddo en internet.

El fallo fue exitoso hacia freddo debido a que freddo es una marca notoria,

estaba bien registrada y la persona que tramitó el dominio de la empresa no pudo

justificar el uso del dominio freddo.com.ar.

**Marca y Patentes**

**Marca**

Signo con capacidad distintiva que permite diferenciar los productos y servicios de una empresa con los de otras empresas a través de la imagen ante los consumidores. Algunas personas resaltan el aspecto psicológico de la marca desde el aspecto experimental. El aspecto

experimental consiste en la suma de todos los puntos de contacto con la marca y se conoce como la experiencia de marca. El aspecto psicológico, al que a veces se refieren como imagen de marca, es una construcción simbólica creada dentro de las mentes de las personas y consisten en toda la información y expectativas asociadas con el producto o servicios.

La diferencia existente entre marca y producto:

● Producto: Es lo que el anunciante fabrica o distribuye y, en definitiva, lo que ofrece a los

consumidores.

● Marca: Es lo que los consumidores compran.

**Patentes**

Una patente es un conjunto de derechos exclusivos concedidos por un Estado al inventor de un nuevo

producto o tecnología, susceptibles de ser explotados comercialmente por un período limitado de tiempo, a

cambio de la divulgación de la invención, o sea una patente de invención es un derecho exclusivo que el

Estado otorga al inventor, a cambio de que éste brinde a la sociedad el fruto de su investigación.

Requisitos para que una invención sea patentable

Una invención debe, por lo general, satisfacer las siguientes condiciones:

● Novedad absoluta: significa que el objeto de invención a patentar no debe estar comprendido

dentro del estado de la técnica conocido, entendiendo por estado de la técnica al conjunto de

conocimientos técnicos que se han hecho públicos tanto en el país como en el resto del mundo,

antes de la fecha de presentación de la solicitud en cuestión.

● Actividad inventiva: Existe actividad inventiva cuando el proceso creativo o sus resultados no se

deduzcan del estado de la técnica en forma evidente para una persona normalmente versada en la

materia técnica correspondiente.

● Aplicación industrial: Habrá aplicación industrial cuando el objeto de la invención conduzca a la

obtención de un resultado o de un producto industrial, entendiendo como industria todo aquello

susceptible de ser fabricado o aplicado.

**Protección del patentamiento**

La protección de una patente significa que la invención no puede ser confeccionada, utilizada, distribuida o

vendida comercialmente sin el consentimiento del titular de la patente.

El cumplimiento de los derechos de patente normalmente se hace respetar en los tribunales que, en la

mayoría de los sistemas, tienen la potestad de sancionar las infracciones a la patente. Del mismo modo, un

tribunal puede asimismo declarar no válida una patente si un tercero obtiene satisfacción en un litigio

relacionado con la patente.

El titular de una patente tiene el derecho de decidir quién puede o no puede utilizar la invención patentada

durante el período en el que está protegida la invención. El titular de la patente puede dar su permiso, o

licencia, a terceros para utilizar la invención de conformidad con términos establecidos de común acuerdo.

El titular puede asimismo puede vender el derecho a la invención a un tercero, que se convertirá en el nuevo

titular de la patente.

La protección es nacional, tanto en Argentina como en el resto del mundo. Esto significa que el solicitante

debe presentar la solicitud de patente en cada país donde le interese protegerla, de acuerdo a las distintas

legislaciones nacionales en vigencia.

**Vigencia de protección de la patente**

La protección se concede durante un período limitado que suele ser de 20 años, luego de ese lapso pasa a

ser de dominio público, ello significa que cualquier persona puede hacer uso de la misma sin tener que

abonar regalías al titular de la patente.

La protección se extingue, por:

● Renuncia de su titular

● Faltar a la ley

● Incumplimiento de la tasa anual

● No uso por dos años.

**Como se concede una patente**

El primer paso para obtener una patente consiste en presentar una solicitud de patente. La misma

contiene, por lo general, el título de la invención, así como una indicación sobre su ámbito técnico; debe

incluir los antecedentes y una descripción de la invención, en un lenguaje claro y con los detalles suficientes

para que una persona con un conocimiento medio del ámbito en cuestión pueda utilizar o reproducir la

invención. Estas descripciones están acompañadas, generalmente, por materiales visuales como dibujos,

planos o diagramas que contribuyen a describir más adecuadamente la invención. La solicitud contiene

asimismo varias “reivindicaciones”, es decir, información que determina el alcance de protección que

concede la patente.

Pasados los 90 días de la fecha de presentación, se realizará un examen preliminar a los efectos de

solucionar posibles defectos formales de la solicitud, en vistas a su publicación. Una vez aprobado el examen

preliminar se publica la solicitud dentro de los 18 meses de la fecha de presentación y luego previo pago de

la tasa correspondiente, se realiza un examen de fondo, a efectos de determinar la novedad de lo

propuesto.

**Obtención del derecho**

Mientras la patente se encuentra en proceso, el solicitante posee un derecho en expectativa. El derecho

sobre la invención recién se otorga cuando la patente se concede. Cualquier conflicto que pudiera surgir

entre un solicitante al que se la ha concedido su patente y un posible infractor que tuviera el producto del

solicitante en el mercado, deberá ser dirimido en el ámbito judicial.

**Modelo de utilidad**

Un modelo de utilidad se otorga únicamente a una disposición o forma nueva obtenida, instrumentos de

trabajo, utensilios, dispositivos u objetos conocidos que se presten a un trabajo práctico, en cuanto

importen una mejor utilización en la función a que estén destinados. En todos los casos, un modelo de

utilidad debe cumplir con dos requisitos de patentabilidad: novedad y aplicación industrial, pero puede no

tener actividad inventiva, ya que este requisito no es obligatorio. Se evaluará que el objeto sea novedoso y

que realmente le sea conferida una mejor “utilidad” por medio de alguna modificación en su estructura, no

importando que dicha modificación sea obvia para una persona del oficio de nivel medio.

**Modelo y Diseño Industrial**

La figura del modelo y diseño industrial está regulada en nuestro país por el decreto ley 6673/63, que

establece que se considera modelo o diseño industrial a las formas o el aspecto incorporados o aplicados a

un producto industrial que le confieren carácter ornamental.

Es el caso de objetos cuyo diseño responde a fines meramente estéticos, sin que necesariamente deba

resolver problema alguno. El modelo industrial es un objeto de tres dimensiones, mientras que el diseño

industrial tiene dos dimensiones y debe ser aplicado a un objeto tridimensional, por ejemplo el entramado

de una camisa o la cuadrícula de un pañuelo o mantel.

**Privatización del conocimiento**

Desde un punto de vista social se argumenta que las patentes de software (y sobre medicamentos, métodos

de negocio, procedimientos legales e ingeniería genética, estas últimas las denominadas patentes de la vida privatizan el conocimiento acentuando las desigualdades sociales y geográficas (ejemplo,

investigaciones en el país, patentadas en el exterior)

**Habeas Data**

**Definición**

La acción de hábeas data es una modalidad de amparo que permite a

toda persona interesada

* Acceder al conocimiento de los datos que consten en registros o

bancos de datos públicos o privados destinados a proveer informes.

* Exigir la supresión, rectificación, confidencialidad o actualización de

estos, en caso de falsedad o discriminación.

Esta información debe referirse a cuestiones relacionadas con la

intimidad y no puede ser utilizada por terceros sin el derecho reconocido

a hacerlo.

**PROTECCIÓN DE DATOS PERSONALES**

DATOS PERSONALES: Son la información de cualquier tipo referida a personas físicas o de existencia ideal

determinadas o determinables

DATOS SENSIBLES: Refiere a los datos personales que revelan origen racial y opiniones políticas,

convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o la vida

sexual.

ARCHIVO, REGISTRO, BASE O BANCO DE DATOS: Conjunto organizado de datos personales que sean objeto

de tratamiento o procesamiento, almacenamiento, organización o acceso.

TRATAMIENTO DE DATOS: Son operaciones y procedimiento sistemáticos, electrónicos o no, que permitan

la recolección, conservación, ordenación, almacenamiento, modificación

RESPONSABLE DEL ARCHIVO, REGISTRO, BASE O BANCO DE DATOS: Es la persona física o de existencia

ideal pública o privada de carácter público, que es titular de un archivo, registro, base o banco de datos.

DATOS INFORMATIZADOS: Son los datos personales sometidos al tratamiento o procesamiento electrónico o

automatizado.

**Puntos interesantes**

Los datos recogidos deben ser ciertos, adecuado y no excesivos para el ámbito donde se van a usar los

mismo

Los datos deben ser exactos y deben poder actualizarse en caso que sea necesario.

No siempre es necesario el consentimiento del titular de los datos, para el tratamiento de los mismos

Ninguna persona puede ser obligada a proporcionar datos sensibles.

Los bancos de datos o bases de datos donde se almacenan los datos deben garantizar seguridad a los mismos.

El titular de los datos, tiene derecho a solicitar y obtener información de sus datos personales incluidos

en los bancos de datos públicos, o privados destinados a proveer informes.

**Derecho a la Intimidad**

El derecho a la intimidad consiste en la defensa de la persona en su totalidad que

prohíbe publicar o dar a conocer datos sobre temas como la religión, la política o la

vida íntima. Todo el ser humano tiene derecho absoluto a mantener su vida privada y

bajo ningún concepto, esto no puede ser revelado.

**Derecho al Olvido**

Hace referencia a la prescripción del dato. Se limita el tipo de información a incorporar a los

archivos:

Solo debe ser aquella relativa a la solvencia económica-financiera y crediticia

Al cumplimiento o no de obligaciones de carácter patrimonial.

Esto evita completar un perfil financiero con información relativa a otras esferas de la vida

personal de las personas.

Esos datos sólo pueden tratarse en todas sus formas si refieren a los últimos cinco años. El

plazo se reduce a dos años cuando el deudor cancele o extinga la obligación.

**Dirección Nacional de Protección de Bases de Datos**

Órgano de control para la efectiva protección de los datos personales.

-Asesora y asiste a los titulares de datos personales.

-Recibe las denuncias y reclamos efectuados contra los responsables de los

registros, o bases de datos por violar los derechos de información, acceso,

rectificación, actualización, supresión y confidencialidad en el tratamiento de

los datos.

Agregue esto