Resumen Aspectos Legales
Parte 2

Clase 7 | Contratos sobre sistemas de información

Contrato de desarrollo de sistemas de información

La adquisición de programas de computadora puede hacer de diferentes modos. En principio, las formas más usuales de contratación son la licencia de uso y el contrato de desarrollo de sistemas a medida.

El contrato de desarrollo se establece habitualmente en los casos de provisión de sistemas a medida, ya sea que estos se desarrollan desde cero o impliquen la adaptación de un software ya existente a las necesidades de un cliente particular. Es lo que se llama software costumisado.

Las características de la figura varían según la relación que se establezca entre el proveedor informático y el usuario. Si entre ellos se establece una relación de dependencia estaremos frente a una relación laboral, constituyéndose el proveedor informático en un empleado del usuario, rigiéndose la relación por las reglas de la ley de contratos de trabajo.

Con respecto al resultado de la obra intelectual, la titularidad en tales casos pertenece al usuario. En tal sentido la ley estipula que se reputaran titulares de la obra “Las personas físicas o jurídicas cuyos dependientes contratados para elaborar un programa de computación hubiesen producido un programa de computación en el desempeño de sus funciones laborales, salvo estipulación en contrario”.

En el caso de grandes emprendimientos es usual que se contrate a una empresa o un trabajador autónomo para que elabore un programa a medida, en este caso, el contrato celebrado será una locación de obra intelectual, obligándose el proveedor a la elaboración de un opus inmaterial, susceptible de entrega. Es el denominado “desarrollo de software”, por el cual se contrata la creación de un programa sujeto a una descripción funcional que la partes acuerdan como anexo al contrato, y que vendría a cumplir una función análoga al plano de una locación de obra material.

Conexo con este contrato pueden existir contratos preparatorios de consultoría destinados a que la empresa que va a hacer el programa determine previamente las necesidades del usuario, factibilidad, costos e impacto que la informatización podría tener en la estructura organizacional.

Respecto del precio, el mismo se puede pactar en un pago único ya sea al comienzo del desarrollo como en la entrega. En los contratos más complejos, el pago suele subdividirse según el cumplimiento de etapas prefijadas del proyecto. En tales casos también es usual la necesidad de agregar funcionalidades al sistema, modificando el desarrollo, por lo que suele preverse la incorporación de nuevas etapas y renegociación del precio.

Si bien normalmente el usuario mantiene la titularidad de la obra, ello no es óbice para que las partes, de así quererlo, reconozcan la titularidad al desarrollador. En tales casos, es norma colocar una cláusula de no competencia para asegurar la inversión del usuario en el sistema.

La entrega final del sistema depende un test de aceptación sobre el sistema instalado y funcionando. En su reglamentación es usual que las partes establezcan un plazo para presentar las objeciones, vencido el cual se da por aprobado el test. Esta convención tiene por objeto evitar la reticencia del usuario en aprobar el sistema, negándose a pagar el saldo de precio y solicitando modificaciones que habitualmente deberían serían objeto de una nueva convención.

La licencia de uso

La licencia de uso es el contrato por el cual titular de un software transfiere a la otra parte, la licenciataria, el uso y goce de sobre el programa.

Desde el punto de vista contractual, no implica la transmisión de un derecho ni produce el cambio de titularidad en forma total o parcial. El productor de software conserva las acciones derivadas de su titularidad, así como la facultad de otorgar a otros la explotación salvo que la hubiera otorgado con exclusividad.

El contrato de licencia es un contrato innominado, dependiendo su contenido de las estipulaciones establecidas por las partes. Tradicionalmente, las mismas otorgan al usuario la posibilidad de utilizar el programa tal cual fue entregado, prohibiendo la modificación del mismo. Tales licencias se conocen como propietarias.

Nada impide que el autor del software lo licencie de forma tal que el propio usuario tenga la posibilidad de modificar el programa y redistribuir la nueva versión. Este tipo de licencia se conoce como licencia de Software Libre o de Código Abierto.

Debe tenerse en cuenta que el carácter gratuito o no de la licencia no es un elemento definitorio en la distinción. Una licencia puede prohibir la modificación del programa y sin embargo distribuirse en forma gratuita o mediante un pago de carácter voluntario. Tal es el caso del Freeware.

Se entiende por código fuente el software escrito en un lenguaje formalizado accesible para el programador, generalmente conocido como lenguaje de alto nivel. El código objeto es la compilación que lo traduce a código ejecutable por la computadora pero incomprensible para el usuario.

De lo expuesto surge claramente que, para modificar el programa original, el usuario necesita el archivo de código fuente, toda vez que el código objeto no permite su alteración por el usuario.

Software Libre y Código Abierto Diferenciaciones ideológicas

El término Software Libre tiene su origen en el manifiesto producido por Richard Stallman en el año 1986, conocido con el Manifiesto GNU. Stallman introduce la licencia GPL, la cual plantea una inversión de los derechos del desarrollador a los efectos de asegurar la libertad de los usuarios la libertad para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software.

El movimiento detrás del manifiesto mantiene un componente ideológico bien determinado basado en la cooperación y la libertad de acceso a la información y el software, que lleva a negar toda restricción a la circulación de copias de productos intelectuales, es el real significado de la expresión “Software Libre”.

En 1997, Eric Raymond publica un ensayo en el que plantea la necesidad de libertad de acceso al código fuente por parte de la comunidad, no desde el punto de vista político sino como

garantía de la elaboración de software de alta calidad, ya que la metodología de trabajo que comenzó con el Kernel de Linux surge como un nuevo de paradigma de desarrollo, que logra resultados en situaciones donde los métodos tradicionales fracasan.

Desde el punto de vista de las definiciones, Raymond prefiere la utilización del término “open source software”, expresión que denota un mayor énfasis técnico que la terminología empleada por Stallman.

El software Libre: las licencias GPL y sus variaciones.

De ambas posturas ideológicas, el Software Libre aparece como la más estructurada desde el punto de vista contractual. La licencia GPL se ha convertido en la más popular forma de licenciamiento y ha evolucionado con el tiempo, encontrándose en la actualidad en su tercera versión.

Tal como han manifestado sus autores, la licencia tiene por objeto habilitar a los usuarios a las siguientes libertades básicas:

1. Usar el programa
2. Estudiar cómo funciona el programa, y adaptarlo a las necesidades de usuario.
3. Distribuir copias.
4. Mejorar el programa y hacer públicas las mejoras.

Formalmente, se divide en tres elementos bien diferenciados, un preámbulo, que expone los principios del movimiento, los términos y condiciones y un apéndice que instruye a los desarrolladores sobre como incorporar a sus programas la licencia GPL.

El preámbulo funciona como una introducción que expresa que el término “free” se relaciona con la libertad concedida al usuario para distribuir y modificar el programa y no por el carácter gratuito del mismo. Al mismo tiempo, establece el concepto de copyleft, como aquellas restricciones en cabeza del usuario creadas con el fin de asegurar la libre distribución de los programas licenciados.

Términos y Condiciones de la GPL versión 3

Ámbito de aplicación

La aceptación de la licencia se produce con la distribución del programa, ya sea en forma original o habiendo producido un trabajo derivado del mismo. Debe tenerse en cuenta que los usuarios no se encuentran obligados a aceptar la licencia para los casos en que su interacción con el programa distribuido se limite a la utilización del mismo o cuando la modificación del mismo no derive en una nueva distribución.

La licencia permite la entrega material del programa a terceros siempre y cuando los mismos actúen por órdenes y en beneficio exclusivo del usuario. En realidad, en tal caso no es posible hablar de distribución, toda vez que los terceros funcionan jurídicamente como una extensión del usuario original, quien los dirige en su propio interés.

Con respecto al objeto de la licencia, alcanza a todo el programa distribuido, pero excluye a los complementos que, si bien pueden interrelacionarse con el software, no se encuentran incluidos en el mismo en su propio diseño.

Distribución del software

Uno de los derechos básicos que otorga la licencia es el de distribuir el programa, siempre y cuando se cumplan las siguientes condiciones:

a) Se deje establecido el copyright original del programa, estableciendo los autores del mismo.
b) Se respete la forma de licenciamiento del programa a distribuir, así como las cláusulas adicionales permitidas por la GPL.
c) Se explicite la inexistencia de garantías establecida por el punto 15 de la licencia.
d) Se acompañe una copia de la licencia junto con el programa.

El distribuidor se encuentra facultado para cobrar por la distribución de así considerarlo conveniente. En tal sentido, la licencia no impone restricciones respecto a los montos o formas de pago que tal operatoria puede utilizar , siempre que las mismas no limiten la posterior distribución del programa en los términos de la licencia .

Es importante señalar que la distribución del programa otorga al tercero receptor una licencia por parte de los autores originales del programa y no del distribuidor. De esta forma, las acciones derivadas por el incumplimiento de las cláusulas contenidas siempre permanecen en cabeza de los primeros, con prescindencia de la forma de adquisición del software por parte del infractor.

Modificación del software

Otra de las libertades básicas de la licencia de software libre es el derecho de los licenciatarios para modificar el programa, adecuándolo a sus necesidades o simplemente optimizándolo. Esta actividad no genera efectos jurídicos de importancia mientras que la modificación no sea distribuida. Si se opta por la distribución de un programa modificado, el licenciatario se encuentra sujeto a una serie de condiciones:

1. Debe establecerse claramente que el trabajo es una distribución modificada del original, estableciendo asimismo la fecha de modificación.
2. Debe notificarse que el trabajo se encuentra distribuido bajo la licencia GPL, como asimismo debe explicitarse cualquier término adicional establecido.
3. En el caso de la existencia de interfaces interactivas debe dejarse en claro los términos de licenciamiento en las mismas.

El programa modificado debe distribuirse como un todo bajo la licencia GPL, aún en los casos en que el mismo se encuentre compuesto por elementos que se hayan licenciado bajo términos diferentes. En los casos que los componentes se encuentren distribuidos en una compilación pero manteniendo su independencia funcional, los mismo pueden ser licenciados bajo términos diferentes.

Desde el punto de vista del derecho de propiedad intelectual, la obra resultante constituye un trabajo derivado del original. Una obra derivada puede ser definida como aquella que depende de un trabajo preexistente, concepto tradicionalmente aplicado a las traducciones o adaptaciones de obras literarias.

Los autores de obras derivadas deben solicitar la autorización del autor original. En el caso de la GPL, la autorización se encuentra contenida en el punto 6 de la licencia siempre sujeta a las condiciones establecidas en la misma. Cumplido este requisito, el autor del trabajo modificado obtiene el derecho de autor sobre este pero no una exclusividad. La ley establece que si bien el autor del trabajo modificado se encuentra protegido, ello no impide que otros terceros

realicen sobre el trabajo original nuevas obras derivadas. Asimismo debe tenerse en cuenta que los derechos se conceden exclusivamente sobre la nueva obra y no afectan los consagrados para el programa original.

Acceso al Código Fuente

En los términos de la licencia, el concepto de código fuente incluye aquellas instrucciones necesarias para generar, instalar y ejecutar el código objeto de un programa determinado. Sin embargo, no incluye las librerías del sistema ni utilidades externas al programa en sí, las que pueden estar vinculadas al mismo, pero no modificadas por este.

Un problema derivado de la nueva redacción de la licencia es utilización del término "bibliotecas compartidas", en particular las llamadas librerías dinámicas. Estas son archivos que contienen código que a menudo es usado por más de un programa simultáneamente, los cuales se limitan a llamar a las funciones de las mismas, sin incorporarlas a su texto.

La licencia determina que se considerará a la biblioteca como parte del trabajo derivado en los casos en que el programa "se encuentre específicamente diseñado para funcionar" con dicha librería .

Por tanto aparece como necesario para mantener la independencia del software creado la existencia de librerías alternativas a la licenciada bajo GPL, de forma tal que las funciones de las mismas sean intercambiables.

Con respecto a la transmisión del código fuente, como principio general, debe estar disponible en los casos de distribución del ejecutable. En los casos de trasmisiones de copias individuales, las mismas deben, en principio, acompañar el código fuente. Excepcionalmente, y solamente con fines no comerciales, es posible acompañar el código objeto con una oferta escrita de proporcionar el fuente correspondiente.

En los casos de distribución digital, el acceso al fuente puede hacerse en el mismo servidor o uno distinto, siempre en cuando las condiciones de acceso sean similares a las utilizadas para distribuir el código objeto.

Una previsión incorporada por la versión 3 es la hipótesis de que el programa sea distribuido como parte de un producto comercial, el cual utilice el software licenciado para su funcionamiento.

En tal caso, el fabricante asume el compromiso de distribuir el código fuente, ya sea mediante la descarga de la versión digital en forma gratuita o el envío de un soporte físico, hipótesis en la que el distribuidor puede solicitar el pago de los gastos. Este compromiso debe extenderse por el plazo de tres años o mientras el distribuidor ofrezca soporte para el producto . Dentro de esta previsión deben incluirse las distribuciones físicas del programa.

Por último, en el caso de distribuciones peer to peer, es obligación de quien realiza la transmisión informar la forma en que se pueda tener acceso tanto en fuente como al objeto.

Copyleft: restricción de licenciamiento de las obras derivadas

El copyleft es definido por la FSF como el método de lograr que un programa sea libre, requiriendo que todas sus distribuciones y trabajos derivados mantengan tal carácter .

Por lo tanto un programa sujeto a Copyleft no puede modificarse ni distribuirse a menos que se haga bajo los términos y condiciones de la GPL, y cualquier modificación a los términos

autorizados por esta última extinguirá los derechos surgidos de la licencia. Jurídicamente, funciona como una “condición resolutoria”.

La existencia del copyleft marca la diferenciación sustancial entre los programas que se encuentran en el dominio público y aquellos sometidos a la licencia de software libre. En estos últimos siguen persistiendo los derechos de autor, que quedan en cabeza del licenciatario original, quien renuncia a los derechos de explotación económica exclusiva de lo creado, sujeto a la condición que los trabajos derivados realicen una similar resignación.

Por lo tanto la vulneración de alguna de las cláusulas entonces resulta violatorio de los derechos del autor del trabajo original.

Cláusulas adicionales

Su objetivo es impedir la creación de otras restricciones distintas a las establecidas por la licencia. Dicha enumeración tiene un carácter restrictivo, por lo que solo se permiten las siguientes estipulaciones:

1. Establecer garantías diferentes a las establecidas en el punto 15 de la licencia.
2. Requerir la preservación de los avisos legales o de autoría contenidos en el programa.
3. Solicitar que las diferencias respecto a la versión original sean señaladas de forma apropiada en las versiones modificadas
4. Limitar el uso de los nombres de los autores originales o licenciatarios para fines publicitarios.
5. Negarse a otorgar derechos afectados por la legislación de marcas comerciales.
6. Prever la Indemnización de los autores o licenciatarios por las distribuciones del programa por parte de terceros que incluyan cláusulas contractuales que impliquen responsabilidad para los primeros.

La aplicación de las dichas cláusulas puede realizarse sobre todo el programa distribuido o sobre parte de él.

Las Patentes de Software

La patente es un mecanismo de protección otorgado por el estado a un particular autor de una innovación tecnológica, por el cual se concede un derecho a la exclusividad a la explotación por un tiempo finito, a cambio de la publicidad de la misma.

Estos derechos se otorgan por cada estado en particular y mantienen a la fecha un carácter marcadamente territorial. Cada estado tiene distintos estándares para otorgar cada patente, en particular en lo que respecta a la patentabilidad del software.

Tradicionalmente, el software como obra intelectual se encuentra protegido por las leyes de derecho de autor.

Algunos países han admitido el patentamiento de los procedimientos realizados mediante un computador, arguyendo que los mismos constituyen una innovación tecnológica similar a cualquier otro proceso industrial.

Debe tenerse en cuenta que a diferencia de los derechos de autor, la patente otorgada no protege el programa de computadora en sí, sino el método tendiente a la obtención del resultado, por ejemplo, la forma de compresión de los datos en un archivo de video.

Consecuencia de ello, la posibilidad de un software alternativo que cumpla la misma funcionalidad sin recaer en la ingeniería inversa, seria igualmente violatoria de la patente otorgada, toda vez que realizaría el mismo proceso, con prescindencia de que se haya o no apropiado del código.

En Estados Unidos de América, el antecedente jurisprudencial permite no solo el patentamiento de invenciones en el sentido clásico del término que incorporen en su diseño programas de computadoras sino asimismo los algoritmos matemáticos que constituyan procesos innovadores cuando estos constituyan una aplicación práctica.

La versión 3 de la GPL da recepción al problema en el punto 11, estableciendo una cesión de la patente expresa por parte de los licenciatarios. Puesto en términos simples significa que si un desarrollador distribuye un programa bajo los términos de la licencia, otorga a los receptores una licencia no exclusiva de todas las patentes que, respecto al programa, pudiera ser titular.

En el mismo sentido, y en los casos en que el distribuidor haya celebrado un convenio de utilización de patentes que sean titularidad de un tercero deberá extender dicho beneficio a los usuarios posteriores o abstenerse de distribuir el trabajo derivado.

Gestión de Derechos Digitales (DRM) y licencias GPL versión 3

Se denomina gestión de derechos digitales (DRM según su abreviatura en inglés) al conjunto de tecnologías que permiten restringir el uso de medios o contenidos digitales a aquellas actividades permitidas expresamente por el titular del copyright. Estas tecnologías pueden estar incluidas en el contenido mismo, en el sistema operativo o incluso en el hardware usado para su reproducción.

Técnicamente, los DRM utilizan dos sistemas para asegurar los contenidos. La primera es la restricción, consistente en aplicar un algoritmo criptográfico al contenido, evitando que los usuarios no autorizados accedan al mismo. El segundo es la aplicación de un “sello de agua” al archivo de forma tal de poder comunicar al hardware que el contenido se encuentra protegido. Ambos casos son susceptibles de acceso no autorizado (hacking) con el fin de eliminar las limitaciones impuestas.

Es por ello que, desde el punto de vista legal, se ha insistido en la necesidad de penalizar los métodos que permitan evitar las restricciones establecidas por el DRM. Es así tal que el tratado de la OMPI del año 1996 aconseja a los países signatarios lo siguiente: "los Estados miembros establecerán una protección jurídica adecuada contra la elusión de cualquier medida tecnológica efectiva, cometida por una persona a sabiendas, o teniendo motivos razonables para saber que persigue ese objetivo", entendiendo por "medidas tecnológicas toda técnica, dispositivo o componente que, en su funcionamiento normal, esté destinado a impedir o restringir actos referidos a obras o prestaciones protegidas que no cuenten con la autorización del titular de los derechos de autor o de los derechos afines a los derechos de autor establecidos por ley".

Los sistemas de DRM han sido objeto de numerosas críticas. Desde el punto de vista de la privacidad, muchos de los sistemas requieren de los usuarios una identificación previa al acceso de los contenidos, excediendo de este modo el mero control de los derechos intelectuales y generando un perfil del propio usuario.

Asimismo, los desarrollos tienden a avanzar sobre los derechos de los propios usuarios consagrados por la legislación de propiedad intelectual. La mayoría de los sistemas restringen

la capacidad técnica de migrar el contenido hacia otros ordenadores propiedad del mismo usuario, así como la utilización de otros sistemas operativos alternativos. De la misma forma, las soluciones adoptadas no discriminan respecto a las excepciones de acceso al material consagradas en la legislación como la utilización con fines didácticos o de investigación.

La versión 3 de la GPL regula los DRM, la distribución de un software bajo esta licencia implica la renuncia a la persecución de la elusión de los métodos de control de contenido establecidos en el software licenciado. Atento la obligación de permitir el acceso al código fuente e instalación de software modificado en los productos de consumo que incluyan software licenciado, los usuarios podrían eludir limitaciones de uso establecidas en los dispositivos sin que ello implique una violación a lo establecido por el acuerdo OMPI.

Compatibilidad con otras licencias GPL

La licencia GPL 3 no está diseñada para reemplazar a las versiones anteriores, por lo que los distribuidores pueden optar por licenciar su código mediante la versión que deseen.

La mayoría de los programas licenciados bajo la versión 2 permiten a los usuarios la posibilidad de modificar los términos de licenciamiento, adoptando la versión 3 de así considerarlo conveniente.

Otras Licencias GPL

La Free Software Fundation promueve otras dos licencias: la Lesser General Public License (LGPL) y la Affero General Public License (AGPL).

La utilización de librerías dinámicas presenta un problema cuando estas se encuentran licenciadas bajo los términos de la GPL, ya que las mismas obligan al programa principal a aceptar estos términos de distribución.

La licencia LGPL aporta una solución al permitir la distribución tanto de la librería como del programa principal bajo términos independientes. Así, el punto 4 permite la distribución de un trabajo combinado que incluya librerías licenciadas junto con el programa principal, siempre y cuando se cumplan las siguientes condiciones:

1. Se deje constancia de la existencia de las librerías y su forma de licenciamiento. Esta noticia debe repetirse en la interfaz de usuario en el caso de que la misma incluya notas de copyright.
2. Acompañar la distribución con una copia de la licencia así como de la GPL.

Con respecto a la obligación de acompañar el código fuente, la obligación se satisface liberando la parte del código correspondiente a la librería incorporada, eximiendo al distribuidor de incluir el correspondiente del resto del trabajo combinado. Debe tenerse en cuenta que por fuente se entiende toda la información necesaria para modificar la librería e incorporarla al aplicativo principal.

La GNU Affero GPL (AGPL) es, en cambio, una licencia destinada a licenciar los programas que utilizan una estructura cliente servidor, típica de las aplicaciones que corren en una red de computadoras.

En términos de su estructura, la AGPL es similar a la GPL versión 3, con la inclusión de un párrafo como punto 13 de la licencia titulado Interacción con redes remotas. Allí se establece el derecho de los usuarios que interactúen mediante una red con el programa licenciado de

obtener una copia del código fuente del mismo, la que debe ser puesta a disposición en un servidor libre de cargo alguno.

La GPL versión 3 prevé en su punto 13 la expresa posibilidad de combinar código distribuido bajo esta licencia con programas sujetos a la AGPL. En tales casos, las previsiones de la AGPL se aplican a todos los programas distribuidos, con prescindencia de su régimen de licenciamiento. De esta forma, la utilización de software licenciado en los términos de la GPL en conjunción con código distribuido bajo licencia Affero, obliga al titular del servidor a poner a disposición de los usuarios remotos la totalidad del código fuente.

Open Software Initiative: Programa de Certificación y Condiciones

A diferencia de los propulsores del software libre, los miembros de la Open Source Initiative no promueven una licencia única sino un programa de certificación de licencias de terceros, las cuales deben cumplimentar los criterios establecidos por la iniciativa. Estos son:

1. Libre redistribución: la licencia no debe impedir a nadie la venta o entrega del software ni requerir derechos de autor u otros pagos por tal venta
2. Código fuente: el programa debe incluir el código fuente, y la licencia permitir la distribución del programa tanto en su versión fuente como en su forma compilada
3. Obras derivadas: la licencia debe permitir la realización de modificaciones u obras derivadas y su distribución bajo los mismos términos de la licencia original
4. Integridad del código fuente del autor: la licencia puede impedir que el código fuente sea distribuido en su versión modificada sólo si permite la distribución de los "parches" (patch files) con el código fuente, con el propósito de modificar el programa en tiempo de construcción. Debe permitir la distribución de software sobre la base de código fuente modificado y puede exigir que las obras derivadas lleven un nombre o número de versión distinto al programa original
5. No discriminación contra persona o grupos de personas
6. No discriminación contra campos de aplicación: la licencia no puede, por ejemplo, impedir el uso del programa en negocios
7. Distribución de la licencia: las facultades concedidas deben ser aplicadas a todas las personas a quienes se redistribuya el programa, sin necesidad de obtener una licencia adicional
8. No especificidad de la licencia con relación a un producto: los derechos aplicados a un programa no deben depender de la distribución particular de software de la que forma parte
9. No restricción de la licencia con relación a otro software: la licencia no debe imponer restricciones sobre otro software que es distribuido junto con el licenciado. Por ejemplo, la licencia no debe insistir en que todos los demás programas distribuidos en el mismo medio deben ser software de fuente abierta
10. Neutralidad tecnológica de la licencia: ninguna de sus estipulaciones puede estar basada en un tipo de tecnología determinado o estilo de interfaz

Toda licencia que cumpla con las condiciones establecidas puede solicitar la certificación de la OSI, la que someterá el pedido a discusión pública, antes de tomar la decisión. En caso que el pedido sea aprobado, la licencia se incorporará al sitio web de la organización y podrá utilizar la marca Open Source Certified.

El objetivo de la certificación es permitir diferenciar las licencias que son realmente open source, logrando una mayor previsibilidad respecto de los alcances de las mismas. En la

actualidad aproximadamente el diez por ciento del software licenciado se hace bajo licencias certificadas, en particular bajo las licencias Apache 2.0 y BSD 2.0.

Una diferencia sustancial con la licencia GPL es la ausencia de Copyleft. En tal sentido, ni las condiciones de certificación ni ninguna de las licencias mencionadas en el párrafo anterior prohíbe al autor de un trabajo modificado la distribución del software bajo una licencia que establezca mayores restricciones, habilitando por tanto la posibilidad de comercializar el producto resultante como software propietario.

Contratos Conexos: El contrato de mantenimiento y escrow de código fuente.

En este sector es habitual hablar de conexidad contractual, denotando que en función de una única operación comercial se celebran una multiplicidad de contratos. El propósito puede ser la informatización de una empresa o sector gubernamental pero esa finalidad se dispersa en una serie de contratos de desarrollo, seguros, financiamiento o asistencia técnica que pueden ser celebrados por distintos proveedores. Entre estos contratos resultan de particular importancia por su especificidad los contratos de mantenimiento y escrow de código fuente.

Junto o posteriormente con un contrato de transferencia de la titularidad del programa informático o la licencia de uso del mismo, es posible celebrar un contrato de mantenimiento. La razón de ser de estos contratos es la complejidad de los sistemas, la multiplicidad de variables a la que están sujetos y como consecuencia de ello, la proliferación de riesgos de todo tipo: desde la simple interrupción del suministro de energía eléctrica hasta la posible irrupción no autorizada en el sistema por parte de un tercero. Para prevenir dichos casos el usuario puede celebrar un contrato de mantenimiento del sistema.

El vínculo puede ser calificado como una locación de servicios profesionales; en cuanto a su objeto son obligaciones de hacer indeterminadas y juzgadas conforme a un estándar profesional.

El contrato de mantenimiento presenta múltiples variables dependiendo de las previsiones del contrato específico y las obligaciones que las partes puedan acordar, pudiendo cubrir desde la mera asistencia ante caídas del sistema a la actualización de los componentes cuando los mismos se tornan inadecuados para el cumplimiento de la función acordada. Estamos ante un estándar abierto de conducta cuya interpretación dependerá en forma sustancial de las previsiones del contrato específico.

Sin embargo debe tenerse en cuenta que desde el punto de vista técnico, la existencia de una licencia propietaria plantea consecuencias de importancia en el contrato de mantenimiento asociado. Toda vez que solo el titular del programa está en posesión del código fuente, las posibilidades de terceros de modificar o resolver problemas sobrevinientes en el sistema se torna nula, debiendo normalmente el usuario celebrar el contrato de mantenimiento con el desarrollador. La falta de previsión al momento de negociar la licencia sin tener en cuenta la celebración del contrato de mantenimiento, puede significar un aumento de los costos posteriores, habida cuenta la mayor capacidad negocial del proveedor derivada del monopolio del código fuente.

Relacionado con el problema del código fuente se encuentra el contrato de escrow. En el caso de licencias propietarias, el código fuente constituye la garantía de exclusividad del proveedor informático, garantía que puede generar problemas al usuario en los casos que el desarrollador se encuentre impedido de prestar los servicios de mantenimiento pactados.

El contrato de escrow se celebra entre la empresa de software propietaria del programa y el usuario con la concurrencia de un tercero depositario del código. El titular de los derechos sobre el software entregará el código fuente al depositario a efectos de que lo conserve en un lugar seguro y lo entregue a las personas designadas en el contrato en el caso de que alguna de las condiciones de cesión establecidas se opere.

Este tipo de contratos es siempre accesorio a otro acuerdo, sea uno de licencia de software, o de reventa de software, etc. Este convenio principal puede realizarse paralelamente al contrato de escrow, con anterioridad al mismo o bien con posterioridad.

Clase 8 | Aspectos legales de Internet

Parte 1: La Internet

"La Internet es una libre asociación de miles de redes y millones de computadoras alrededor del mundo, que trabajan juntas compartiendo información".

La Internet constituye una red de carácter descentralizado y redundante. Descentralizado, toda vez que no existe un punto central de concentración de la información, sirviendo cada uno de los nodos de la red como un servidor. Redundante, porque las conexiones entre los distintos elementos no son únicos sino que pueden ser suplantados por otras rutas de conexión, de forma tal que la caída de uno o varios de los servidores no impide el acceso la información contenida en el resto de los servidores que conforman la red.

Un protocolo de comunicación es una forma standard de transmisión de datos entre dos máquinas de forma tal que tanto la receptora como la emisora puedan entender y decodificar el mensaje.

En el caso de la Internet, nos encontramos ante dos protocolos: el TCP o protocolo de control de transmisión y el IP o protocolo de Internet.

El primero de ellos deconstruye el archivo a enviar en una serie de elementos menores o paquetes de información los cuales viajan por la red hasta la computadora de destino donde el TCP de esta última vuelve a ordenar los paquetes a los efectos de obtener el archivo original.

La forma en la que estos paquetes de información viajan es mediante el IP o protocolo de Internet. El mismo envía paquetes de información a través de la red mediante la elaboración de guías donde se establece una ruta a través de los distintos servidores.

Internet y World Wide Web

Internet ≠ WWW

La Internet constituye una red global de computadoras de carácter descentralizado. La Web, en cambio, es un subconjunto de la misma, un grupo de documentos que trabajan utilizando un standard específico: el protocolo de transferencia de hipertexto o HTTP.

La Web trabaja sobre una serie de documentos que se relacionan entre sí, formando lo que comúnmente se conoce como "paginas" las cuales no son otra cosa que un conjunto de ordenado de archivos los cuales son accedidos a través de los llamados "hipervínculos" o "hipertextos".

Hipertexto es un texto que contiene una conexión o "link" a otro documento. Este permite acceder rápidamente a la información relacionada con el texto que se está leyendo. Esta

información puede está contenida en el mismo archivo o en otro ubicado incluso en un servidor diferente.

La forma en la que se programan estos hipertextos es por medio del HTML o lenguaje de adiciones de hipertexto. El mismo consiste en un conjunto de instrucciones relativamente sencillo a los efectos de definir como se estructura la página. Fundamentalmente, define cuales son los bloques de texto que componen cada documento, así como cuales son las conexiones que deben realizarse a los efectos de incorporar archivos de otros medios o remisiones a otras páginas. El browser interpreta los comandos de HTML que recibe y presenta el documento formateado.

Efectos Jurídicos de la Internet

El control sobre la red: La sociedad de Internet

La Corte Suprema de los Estados Unidos sostuvo que "Ninguna persona, compañía, institución u organización gubernamental es dueña de Internet, ni tampoco lo gobierna, o incluso tiene un interés controlante".

Ello no implica que la red carezca de control, la Sociedad de Internet es una organización no gubernamental, sin nacionalidad definida ni fines de lucro. Está formada por organizaciones de ciento sesenta y cinco países, cuenta con más de ocho mil miembros, los cuales trabajan elaborando políticas y prácticas para ser adoptadas por la red, como asimismo supervisan el trabajo de las organizaciones, grupos de tareas, que trabajan en las decisiones políticas de la red.

Entre las organizaciones que se encuentran bajo la supervisión de la Sociedad de Internet se encuentran:

1. IAB (Junta de Arquitectura de Internet): es el grupo de consultores técnicos de la Sociedad de Internet. Son sus responsabilidades:
    a. Nombra a las autoridades del IETF y a los miembros del IESG.
    b. Vigilancia de los standards de proceso y apelación: supervisa los procesos a los efectos de crear los standards de Internet. Además, actúa como un consejero de apelación respecto a las divergencias respecto a la ejecución de dichos standards.
    c. Nombres de Dominio: asigna y controla los nombres de dominio de primer orden.
    d. Representación: representa a la Sociedad de Internet en las cuestiones atinentes a standards y cuestiones técnicas en los casos que estas repercutan en la red.
    e. Asimismo la IAB tiene bajo su supervisión una serie de organizaciones en las que podemos mencionar:
        i. IANA (Autoridad de Asignación de Números): es el organismo encargado de otorgar los nombres de dominio en Internet.
        ii. IEFT (Grupo de trabajo de Ingeniería de Internet): es la encargada del desarrollo de los protocolos de Internet.
        iii. IESG (Grupo de dirección de Ingeniería de Internet): es el responsable de la del manejo técnico de las actividades de Internet.

2. IRFT (Grupo de Trabajo de Investigación de Internet): es el organismo encargado de la investigación respecto a los aspectos técnicos de la Internet, para lo cual cuenta con grupos de estudio.
3. ISTF (Grupo de Trabajo Social de Internet): es el organismo encargado de la elaboración de las políticas tendientes al máximo aprovechamiento social de la red, entendiendo al mismo como posibilidad de todos los habitantes de acceder a la red.

El problema de la jurisdicción en Internet

Debe tenerse en cuenta que cualquier acto o hecho jurídico llevado a cabo en la red, los participantes del mismo pueden estar ubicados en varios países del mundo. Del mismo modo, el servidor en el que estas personas interactúan puede estar ubicado en un tercer lugar. El problema del derecho, entonces, consiste básicamente en determinar cuál es la legislación aplicable, así como la jurisdicción aplicable tanto en etapa de conocimiento como de ejecución.

Si bien es práctica común en la mayoría de los contratos celebrados por Internet la inclusión de cláusulas que definan jurisdicción y normativa aplicable, la mayoría de estos actos jurídicos constituyen convenios de adhesión, lo que implica el riesgo jurídico que dichos acuerdos carezcan de validez por ser considerados nulos en los casos que impliquen un injustificado beneficio.

La solución de considerar el domicilio del servidor a los efectos de la jurisdicción, presenta numerosos inconvenientes, siendo quizás el más importante la posibilidad de creación de "servidores de conveniencia", es decir el desplazamiento de la jurisdicción y legislación aplicable a una más conveniente mediante el mero traslado del computador a un territorio ajeno por completo a la explotación o intereses de la empresa prestataria del servicio.

La solución contraria, otorgar la jurisdicción en el territorio del reclamante, no está tampoco exenta de problemas, toda vez que somete a la empresas y particulares que utilizan la red al riesgo de verse sometidos a cualquier régimen jurídico o jurisdiccional sin posibilidad de control alguno.

Si bien el problema no ha obtenido una respuesta definitiva, una de las soluciones más aceptadas es la aplicación de la doctrina del Long Arm.

En dicho caso, un proveedor de Internet de Nueva York demando por violación de marca a un segundo proveedor, el cual si bien tenía su domicilio en Georgia, ofrecía sus servicios mediante su página web a personas indeterminadas, incluidas los habitantes del estado de Nueva York . El demandante sostenía la jurisdicción de los tribunales de Nueva York, pretensión que fue admitida merced a los siguientes argumentos:

1. Si bien el demandado cometió el hecho en otro estado, el demandado sufrió un daño en el de Nueva York, al ser confundida su marca con la perteneciente a la pasiva.
2. Era previsible para el demandado que su actividad tuviera repercusiones en Nueva York, toda vez que ofreció su servicio a clientes de todo Estados Unidos y había aceptado suscriptores en dicho estado.
3. Merced a dicha actividad el demandado recibió un rédito mensurable, circunstancia que no fue rebatida por el mismo.

En virtud de ello, la corte entendió que la jurisdicción se encontraba habilitada. Por tanto y a los efectos de cerrar el tema enunciaremos la regla del Long Arm:

- La Corte puede ejercer la jurisdicción personal sobre cualquier no residente que cometa un acto delictivo fuera del Estado causando daño a personas o propiedades dentro del estado, si él pudo esperar o razonablemente debió prever que el acto tenga consecuencias en el Estado y obtuvo un beneficio sustancial del comercio interestatal o internacional.

Parte 2: Régimen Legal del Nombre de Dominio

Nombre de dominio: cualquier designación alfanumérica que se registra o asigna y forma parte de una dirección electrónica.

Las direcciones en Internet se expresan mediante una secuencia identificatoria de números separados por períodos o campos, sin embargo, este sistema es altamente engorroso para el usuario medio de la red, por lo que esta secuencia puede ser traducida o asociada a una expresión alfanumérica de forma tal que sea más sencillo de recordar.

Por tanto las direcciones numéricas son traducidas mediante un sistema de nombres de dominio conocido como DNS en una expresión alfanumérica. Esta solución técnica, que permite un mejor acceso a la red, implica una serie de problemas jurídicos, toda vez que los distintos emprendimientos han intentado vincular sus nombres de dominio a sus marcas comerciales, a los efectos de beneficiarse con las campañas de Marketing elaboradas en el mundo real.

El DNS. Funcionamiento. Principios.

El DNS es un protocolo de traducción de identificaciones numéricas en una cadena alfanumérica que pueda ser fácilmente recordada por el usuario. Sin embargo, dicha cadena alfanumérica no es uniforme y presenta distintos elementos cuya protección jurídica es disímil. Tomemos el ejemplo:

- http://www.cnet.com

En la dirección podemos ver dos elementos diferenciados: Una parte exclusiva (CNET) y otra genérica como es la expresión ".com". Este último elemento, conocido como dominio genérico, carece de la protección otorgada al elemento especifico, toda vez que constituye una convención aceptada por todos los usuarios de la red que en el caso particular denota que se trata de un sitio comercial.

Con respecto a dichas convenciones, las mismas se pueden dividir en dos grandes grupos según que su registración se encuentre limitada o no. Entre aquellos dominios genéricos reservados podemos nombrar a ".gov" para organismos de gobierno, ".int", para organismos supranacionales y "mil" para entidades militares. En los dominios libres se encuentran ".com" (empresas comerciales), ".net" (redes informáticas) y ".org" para entidades sin fines de lucro y asociaciones en general.

A los efectos de la diferenciación de las distintas páginas se han agregado los genéricos geográficos, los cuales son normalmente administrados por una entidad local. Por ejemplo, supongamos que el sitio anterior abriera una filial para la argentina y otra en brasil, lo que crearía dos nuevos nombres de dominio:

- http://www.cnet.com.ar
- http://www.cnet.com.br

Estas dos nuevas siglas denotan la nacionalidad del sitio.

Administración de los nombres de dominio. Su registración.

El Régimen Argentino de nombres de dominio se encuentra regulado por un organismo internacional y otro nacional con competencia exclusiva en lo que respecta a los dominios .ar.

En la República Argentina la regulación plantea un sistema laxo en lo referente a los requisitos y formalidades necesarias para la inscripción del nombre de dominio. El registro del nombre de domino se realiza mediante un formulario electrónico disponible en el sitio Web de Nic-Argentina, el cual cumple la doble función de declaración jurada respecto de los datos a ingresar y aceptación de los términos y condiciones.

El sistema utilizado para la registración en estos casos sigue el principio de "primero en el tiempo, primero en el derecho", sin que la autoridad de aplicación realice un examen exhaustivo de la legalidad del uso del nombre. De esta forma, Nic-Argentina elude toda responsabilidad derivada de daños por violación a la ley de marcas o cualquier otro perjuicio a terceros, quedando en cabeza del registrante dichos riesgos. Sin embargo, y excepcionalmente, es facultad de Nic-Argentina la posibilidad de rechazar una petición por considerar que la misma implica la violación flagrante de una marca conocida o una invasión a la privacidad de una persona física.

Los únicos límites impuesto por la reglamentación son los derivados de la moral y las buenas costumbres y la imposibilidad de registrar nombres de dominio ya existentes. Como excepción, se impide el registro de nombres de dominio que se correspondan con organismos estatales o aquellos que lleven el genérico .GOV los cuales corresponden a reparticiones estatales y conllevan un sistema de registro un poco más complejo.

El registro del nombre de dominio es válido por un año renovable, sin que exista límite a la cantidad de veces que esta facultad se utiliza.

La relación entre el nombre de dominio y las marcas comerciales : El cybersquatting.

Si bien en numerosas ocasiones se han equiparado el nombre de dominio a una marca comercial, los primeros presentan características distintivas.

En primer lugar, la protección otorgada a las marcas comerciales mantiene una doble limitación: en un aspecto material, imposibilita solamente la utilización de homónimos respecto a productos similares o que de alguna manera puedan ser relacionados con la marca protegida, y en el ámbito territorial la prohibición se circunscribe solamente al territorio del país donde de la marca sea a registrado. Los nombres de dominio, en particular los de primer orden, carecen de esta diferenciación, mientras puede haber varios negocios llamados Gomez dentro de un mismo territorio, siendo uno dedicado a la cría de ganando y el otro a la venta de artefactos de baño, el nombre de dominio www.gomez.com es único para todo el orbe e impide diferenciar cuales son las actividades realizadas por el titular.

En segundo lugar, las marcas mantienen una identidad iconográfica de la que carecen los nombres de domino: mientras la marca Coca Cola mantiene un logotipo y tipografía identificable, propia y susceptible de defensa jurídica, el nombre de dominio http://www.cocacola.com no resulta modificado por la tipografía o características gráficas utilizadas para su inclusión en el browser.

Por último, mientras que las marcas denotan la existencia de productos en el mercado, los nombres de dominio no necesariamente implican una actividad comercial, pudiendo ser simplemente páginas personales o sin ningún tipo de interés comercial.

Por lo tanto, no es posible asimilar los nombres de dominio a las marcas comerciales, lo cual, sin embargo, no impide que entre ambas figuras se produzcan relaciones. Tal como ya adelantamos, es innegable el beneficio que para las empresas significa el aprovechamiento del prestigio de sus marcas comerciales en sus estrategias en la Web, interés que puede verse frustrado por el mero registro del nombre de dominio por parte de un tercero con la única intención de lucrar con su venta. Esta práctica, lamentablemente, se ha vuelto tan común que ha recibido un nombre para identificarla: Cybersquatting.

En la república argentina, si bien no existe todavía una legislación las vías procesales utilizadas a los efectos de la solución de los conflictos que se han suscitado han sido tanto la judicial como los procesos arbitrales ofrecidos por el NIC-Argentina.

Las experiencias jurisprudenciales argentinas presentan la particularidad de carecer de sentencia firme. Por ejemplo en Freddo S.A. c/Spot Network la mera inclusión de una marca comercial implica necesariamente una infracción sancionable, pero en otros casos como el de Pugliese, Francisco c/Perez, Carlos, no parece tan claro, toda vez que los elementos varían, no existe una marca claramente reconocida en el mercado que necesariamente implique una privación de ganancias por la imposibilidad de explotación. En segundo lugar, en este caso el titular del dominio se encontraba utilizando el mismo a los efectos del mantenimiento de una página personal, la que coincidía con las siglas de su nombre.

En lo que respecta a las soluciones arbitrales, las mismas encuentran su fundamento en una cláusula compromisoria elaborada por la IANA, el régimen esta dado por un documento denominado Política Uniforme de Solución de Controversias en Materia de Nombres de Dominio y su respectiva reglamentación. Sus principales características son:

1. Es un proceso voluntario: tanto para el demandado que acepta el mismo en momento del registro como para el demandante, quien lo hace al momento de iniciar el procedimiento.
2. Permite un conocimiento pleno: más allá de las características que cada proveedor le otorgue a través de su reglamentación, ambas partes deben ser oídas mediante una demanda y su contestación.
3. Es arbitral: la cuestión es resuelta mediante laudo fundado emitido por un tribunal unipersonal o colegiado de expertos en la materia.
4. Es obligatorio: la resolución arribada tiene carácter obligatorio para las partes

La Política Uniforme de Solución de Controversias en Materia de Nombres de Dominio define claramente cuáles son los extremos a acreditar al momento de acreditación de la demanda:

1. El nombre de dominio registrado debe ser idéntico o similar, hasta el punto de crear confusión con respecto a las marcas de productos o servicios sobre los que el demandante tiene derechos. Debe tenerse en cuenta que los nombres personales cuando los mismos son lo suficientemente conocidos pueden asimilarse a una marca comercial.
2. El titular del nombre de dominio carece de título o interés legítimos respecto al nombre de dominio en cuestión.

3. El nombre de dominio ha sido registrado de mala fe. Se han entendido que constituyen indicios de mala fe:
    a. El registro con propósito de venta del nombre de dominio.
    b. El registro a los efectos de impedir el uso normal de la marca, cuando esto constituya un patrón de conducta.
    c. El registro de marcas de la competencia al solo efecto de entorpecer su giro normal.
    d. El intento de atraer visitantes con fines comerciales, sacando provecho de la confusión con la marca comercial.

Parte 3: Responsabilidad Civil en Internet

Proveedores de Acceso a Internet

Los proveedores de acceso son los sujetos jurídicos que prestan la infraestructura técnica para que los proveedores del servicio de Internet ofrezcan su servicio. Los proveedores carecen de control y acceso a los contenidos que circulan por la web, por lo que no podría reputárselos responsables civiles de los mismos.

Servicios de Caching

El servicio de caching almacena en forma automática, provisional y temporaria cierta información con el único fin de que sea más eficaz la transmisión la misma.

En principio carecen de control sobre el contenido de almacenado, por lo que se les debe eximir de responsabilidad.

Sin embargo, es posible que el proveedor de caching tenga acceso al contenido o capacidad para controlarlo o modificarlo. En tales casos la eximente de responsabilidad desaparece.

Proveedor de Contenido

Entendemos por proveedor de contenido todo aquel que coloca archivos informáticos en la web con el fin de que terceros accedan a ellos.

Sobrino diferencia entre los productores de contenido según que los mismos creen contenidos propios o refieran a contenidos ubicados en páginas realizadas por terceros. En el primero de los casos la responsabilidad del proveedor de contenido es clara, atento el carácter de autor del contenido. La cuestión es más compleja en los casos de referencia a material de tercero.

Técnicamente, la forma de referir a material de terceros es la generación de hipervínculos a la dirección de Internet donde se encuentra disponible el mismo. A su vez, esta página puede contener nuevos links a otros sitios de Internet y así sucesivamente. Por tanto podemos diferenciar entre contenidos indirectos de primer nivel y de segundo, sea que el acceso se produjo desde la página original o desde la referida.

Desde el punto de vista de la responsabilidad parece clara la obligación de responder del proveedor de contenido por los contenidos de primer orden. Si bien no es el autor, el proveedor de contenido realiza una acción voluntaria al vincularse al contenido objetable, permitiendo el acceso desde su sitio a los terceros.

Con respecto al contenido de segundo orden, extender la responsabilidad respecto de los mismos aparece como excesivo atento la inexistencia de un control o conocimiento directo del proveedor de contenido.

Proveedores de servicio de Internet

Se entiende por proveedor de servicio de Internet a los sujetos jurídicos que permite a los usuarios particulares acceder a la Internet. Asimismo y en forma habitual, el proveedor de Internet (ISP en inglés) ofrece servicios de Hosting, permitiendo a los usuarios colocar contenido en Internet a disposición de terceros.

La Directiva Europea establece la ausencia de responsabilidad de los proveedores de hosting mientras el mismo no tenga conocimiento efectivo de la actividad ilegal. En el mismo sentido, Estados Unidos consagra la inmunidad.

Jurisprudencialmente, los tribunales han consagrado la responsabilidad de los ISP en la hipótesis que estos, teniendo conocimiento de la actividad ilícita omitan tomar las medidas necesarias para poner fin la misma.

La cuestión en la argentina: El caso Jujuy.com

La empresa Jujuy digital operaba el dominio Jujuy.com, en cuyo foro se publicó en forma anónima un mensaje respecto de la supuesta infidelidad de dos actores. Este mensaje fue retirado luego de que el sitio recibiera intimación por carta documento, circunstancia que fue considerada una conducta omisiva por el tribunal y un reconocimiento de la actividad ilícita.

En sus considerandos el tribunal entendió que una vez demostrada la existencia del daño, la responsabilidad surgía en forma clara. Se sostiene la analogía con la energía en cuanto al material riesgoso, considerando procedente la responsabilidad objetivo de los codemandados por los daños producidos.

El fallo merece una serie de críticas. En primer lugar, la aplicación de los criterios de responsabilidad objetiva está apartada de la legislación y jurisprudencia comparada, creando un posible riesgo jurídico para las empresas que prestan servicios de hosting o simplemente permiten a los usuarios expresar una opinión. En segundo lugar, la analogía utilizada no aparece como la más feliz. El análisis realizado establece un doble estándar de responsabilidad según si el mensaje fue realizado mediante un medio tradicional o vía web, ignorando el hecho que el daño se produce por la existencia del mensaje y no por la utilización de la herramienta informática.

Clase 9 | La Firma Digital

La Firma Digital

El Código Civil establece como requisito de los instrumentos privados la firma que tiene dos requisitos, la habitualidad y la intención de manifestar el consentimiento. La firma constituye un mecanismo que permite identificar a los autores de un escrito e imputar el contenido del mismo a esta persona.

La firma de puño y letra de una persona contiene una serie de variables (caligrafía, inclinación del instrumento de escritura, presión ejercida sobre el papel) que se mantienen constantes y permiten al observador entrenado comparar distintas signaturas determinar la autoría de una firma.

Con la intención de digitalizarla, atento la inexistencia de un formato papel, resulta imposible la escritura de puño y letra, requisito indispensable para la firma ológrafa.

Resulta entonces indispensable encontrar otro método de autenticación de los mensajes, que permita identificar a sus autores sin necesidad de un soporte material. Allmark y Bergel señalan que existen tres clases de formas de autenticación de los documentos electrónicos:

1. El código de ingreso**:** está compuesto de una combinación determinada de cifras o letras, solo conocidas en principio por el titular del mismo. Son asimismo denominados por la doctrina como P.I.N. (Personal Identification Number).
2. Los métodos biométricos**:** son aquellos que utilizan las características fisonómicas únicas de cada sujeto para su identificación. Dentro de esta categoría podemos incluir a los lectores de retinas y huellas digitales, así como a los sistemas de reconocimiento de voz.
3. Los métodos criptográficos: utilizan métodos matemáticos de codificación de los mensajes para lograr determinar la identidad del autor del mensaje.

En cuanto a los métodos criptográficos, los elementos básicos del sistema son un método de cifrado y una clave para su decodificación. En la búsqueda del método más eficiente se encontró un algoritmo que utilizaba dos claves, una pública y otra privada. La comunicación entonces podría ser cifrada con la clave pública por cualquier persona, pero solamente podría ser desencriptada por el dueño de la clave privada, asegurando la confidencialidad del mensaje. Asimismo, si se desea asegurar la autoría, es necesario invertir los términos del algoritmo: si codifico el mensaje con mi clave privada, entonces solo yo puedo ser el autor del mismo.

Sin embargo, el problema de utilizar esta forma de encriptación es doble: En primer lugar, el receptor no puede asegurar que el mensaje haya sido modificado, atento que para su lectura solo hace falta utilizar una clave conocida por todos. En segundo lugar, salvo que exista un acuerdo anterior con el emisor, no es posible determinar a ciencia cierta quien es el autor del mensaje. El primero de los problemas se soluciona con la aplicación de un nuevo algoritmo matemático conocido como Hash. Un hash puede ser definido como un número que se obtiene haciendo una operación matemática sobre todos los caracteres del mensaje.

El segundo problema se basa en la imposibilidad de acreditar la identidad de remitente. Salvo que las partes hayan acordado usar una clave determinada, no es posible conocer cuál es la clave pública correspondiente al mensaje y aun en la hipótesis que la conociéramos, de ello solo podemos derivar, más allá de toda duda, una correspondencia entre ambas claves, pero no respecto a la identidad de quien la envía. Se hace necesaria la intervención de un tercero confiable que acredite esta identidad mediante la expedición de un certificado digital que acompañe al mensaje, para así vincular jurídicamente el mensaje con su autor.

Por lo tanto, el problema de la regulación de la firma digital conlleva el análisis de tres cuestiones básicas: El concepto mismo de firma, o dicho de otro modo, cuáles son las tecnologías que recepta el ordenamiento como forma de acreditación de la identidad; los efectos jurídicos que le otorgan al documento resultante y por último cuál es la estructura de certificación que nos permiten imputar un mensaje a una persona determinada.

Concepto Legal de Firma: La Firma Digital y Firma Electrónica.

“Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar

cualquier alteración del documento digital posterior a su firma. Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes"

Si bien de la definición no establece en forma expresa la adopción de la criptografía asimétrica como tecnología utilizada para la firma digital, manteniendo una nominal neutralidad tecnológica, de la descripción utilizada resulta clara su adopción como medio de identificación del firmante.

La firma electrónica es una definición residual entendiendo por tal aquellos medios de identificación electrónicos que no cuenten con las previsiones prescriptas por la ley para ser considerados firma digital. La firma digital, al exigir mayores requisitos, obtiene un mayor nivel de seguridad, que permite las presunciones respeto de la autoría y la integridad del mensaje.

La directiva europea habla de firma electrónica y electrónica avanzada, siendo esté último término equivalente a nuestra firma digital. Estados Unidos define a la firma electrónica como un proceso electrónico que permite imputar la manifestación de voluntad de una persona determinada, evitando cualquier categorización y manteniendo una verdadera neutralidad tecnológica. La solución argentina no aparece como la más acertada, es criticable la redacción de la firma electrónica toda vez que define un instituto de forma subsidiaria, omitiendo enunciar sus condiciones necesarias. Dicho de otro modo, la firma electrónica se encuentra definida por lo que no es y no por lo que es.

En cuanto a la validez de la firma digital, el art. 3 asimila la firma digital a la ológrafa. La utilización del término firma digital dio pie a la discusión respecto si el requisito de la firma quedaba satisfecho con la utilización de la firma electrónica, el decreto 2628/02 establece que pueden utilizarse cualquiera de las dos soluciones tecnológicas.

El art. 4 establece las excepciones al principio de equivalencia: las disposiciones por causa de muerte, los actos jurídicos del derecho de familia y los actos personalísimos en general y aquellos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea que la incompatibilidad nazca de la ley o del propio acuerdo de partes. El fundamento de dichas hipótesis se funda en la necesidad de una seguridad calificada que a criterio del legislador solo puede quedar asegurada mediante la firma ológrafa.

Documento electrónico

Se lo define como la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo.

Allmark y Bergel definen al documento electrónico como aquel gestado con la intervención de un ordenador. En tal sentido, el mismo puede estar sobre un soporte volátil, como la memoria RAM de una computadora o en un medio destinado a permanecer inalterable, como en el caso del almacenamiento óptico (CD-ROM o DVD).

En los casos de formatos que permitan asegurar la permanencia, resulta claro que el mismo puede admitirse como una prueba documental, similar a una fotografía o una cinta de audio. Sin embargo el tráfico jurídico necesita una mayor seguridad, debiendo equiparse el documento digital al instrumento privado o público según el caso.

Para el exista escritura es necesario que nos encontremos frente a un mensaje escrito en un soporte que permita la conservación, en un lenguaje destinado a la conservación. Todos estos elementos se encuentran en el documento electrónico.

El art. 6 actualiza la definición del código civil, desvinculando el mensaje de la tecnología utilizada para su conservación. Es así que permite asimilar la representación digital al concepto de instrumento al momento que establece in fine que "Un documento digital también satisface el requerimiento de escritura".

Según lo normado por el Código Civil, los instrumentos privados necesitan el reconocimiento de quien lo suscribió para obtener capacidad probatoria, en el caso del firmante de un documento, es obligación el reconocimiento del mismo en caso de ser presentado en juicio, recayendo la carga de la prueba de la autoría en quien presenta el mismo. En el caso de los documentos firmados digitalmente este criterio se encuentra modificado, ya que el método de criptografía asimétrica permite asegurar no solo la autoría del documento enviado sino asimismo la inalterabilidad del mensaje.

Es por ello que la ley establece la presunción de la autoría del documento en los siguientes términos: Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma. En similares términos el art. 8 establece la presunción Iuris tantum respecto de la inalterabilidad del documento.

Esta presunción se establece solamente respecto de la firma digital. La firma electrónica, atento los menores niveles de seguridad que ofrece, se asimila a la ológrafa siendo necesaria la prueba de su autoría en el caso de desconocimiento.

Ello deriva en una inversión en la carga de la prueba en los casos de la firma digital, recayendo en quien desconoce la autoría o integridad del mensaje, la actividad tendiente a logar el convencimiento del juez respecto a la falsedad alegada.

Con respecto a la existencia de múltiples ejemplares del documento, debe tenerse en cuenta que desde el punto de vista técnico no existe diferencia entre el original digital y las subsecuentes copias que de él se extraigan. Este es el fundamento del texto del art. 11 que equipara al original los documentos digitales de segunda generación, obteniendo el mismo valor probatorio.

El Certificado Digital

El certificado digital cumple una función fundamental en la identificación del remitente del mensaje.

Al mismo tiempo, esta función conlleva la potencialidad de generar grandes perjuicios para los tenedores de certificados en los casos de certificadores negligentes o malintencionados. Es por ello que la ley de firma digital establece el control de la actividad por parte del estado, quien regula las condiciones que deben cumplir las empresas que deseen prestar el servicio.

Es definido como "el documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular". Técnicamente, constituye un mensaje que se adjunta al principal, en el que constan los datos del remitente, como asimismo los elementos necesarios para determinar los alcances de la firma otorgada.

Los certificados digitales deben cumplir los siguientes requisitos:

1. Ser emitidos por un certificador licenciado por el ente licenciante;

2. Responder a formatos estándares reconocidos internacionalmente, fijados por la autoridad de aplicación, y contener, como mínimo, los datos que permitan:
    a. 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;
    b. Ser susceptible de verificación respecto de su estado de revocación;
    c. Diferenciar claramente la información verificada de la no verificada incluidas en el certificado;
    d. Contemplar la información necesaria para la verificación de la firma;
    e. Identificar la política de certificación bajo la cual fue emitido.

El primero de los requisitos es la necesidad de que los emisores de certificados digitales encuentren licenciados por el estado. El decreto 2628/02 establece la diferenciación entre los certificados digitales emitidos por certificadores licenciados y los emitidos por los que carecen de tal condición. El art. 3 del reglamento otorga a los documentos firmados con los primeros las presunciones contenidas en los artículos 7 y 8 de la ley de firma, mientras que la ausencia de licenciamiento por parte del estado transforma a las firmas utilizadas en simplemente electrónicas.

Hay que tener en cuenta cuales son los actos que permite realizar el certificado, la ley resta validez a los actos realizados fuera de los parámetros autorizados por el certificado, ya sea porque su objeto es manifiestamente extraño o porque el mismo excede los montos autorizados.

Respecto a la eficacia del certificado, el art. 15 de la ley ordena que los mismos solo serán válidos dentro del período de vigencia, el cual debe ser indicado en el mismo, consignándose tanto la fecha de inicio como la de vencimiento.

Asimismo, y aún antes de su vencimiento, los certificados pueden ser revocados en los supuestos contemplados por la ley, la ley de firma enuncia los casos en que el certificador tiene la obligación de dar de baja el certificado. Las hipótesis son:

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.

Además hay un decreto que agrega:

1. Muerte o desaparición con presunción de fallecimiento.
2. Si la firma se ha otorgado en razón de un mandato y este se ha revocado.
3. En los casos de la información suministrada haya dejado de ser válida.

Con respecto a los certificados expedidos en el extranjero, estos podrán ser reconocidos en dos casos, si existe un acuerdo de reciprocidad firmado por la República Argentina y el país de origen del certificador o en la hipótesis que el certificador extranjero sea reconocido por un certificador licenciado previa validación de la autoridad de aplicación.

Certificadores licenciados y autoridades de registro

Los certificadores licenciados son definidos en el art. 17 de la 25.506 como las personas de existencia ideal, registro público de contratos u organismo público autorizado para actuar como proveedores de servicios de certificación en los términos de la Ley 25.506 y su normativa.

El certificador debe obtener una licencia (Art.20) para lo cual debe cumplir con los requisitos exigidos por la ley y tramitar la solicitud respectiva. La licencia le será otorgada previo dictamen legal y técnico que acredite la aptitud para cumplir con sus funciones y obligaciones.

El certificador debe cumplir una serie de funciones, recibir solicitudes de emisión de certificados digitales, emitir certificados digitales, y controlar los mismos, manteniendo copias de todos los certificados emitidos. Son asimismo los encargados de revocar los certificados digitales que hayan emitido.

La ley reconoce un tipo especial de certificado denominado Certificado por Profesión el cual puede ser emitido solamente por las entidades que controlan las matrículas profesionales, respecto de sus afiliados, las cuales tendrán la misma validez que la firma manuscrita.

El decreto reglamentario 2628/02 en su Art. 35 crea la figura de la Autoridad de Registro con la función específica de validar la identidad. Los Certificadores Licenciados podrán delegar en ellos las funciones de validación de identidad y otros datos de los suscriptores de certificados. Dichas Autoridades están igualmente autorizadas para el archivo y la conservación de toda la documentación respaldatoria del proceso de validación de identidad.

Debe tenerse en cuenta que la utilización de los servicios de la autoridad de registro no implica una limitación de la responsabilidad de los certificadores licenciados, los que siguen siendo responsables por los daños derivados de los errores contenidos en los certificados por ellos emitidos.

Estructura Administrativa de firma digital en la ley 25.506

Podemos definir a la estructura administrativa como el conjunto de organismos del estado encargados del control del servicio de gestión de certificados.

La normativa vigente establece la configuración de una Infraestructura de Firma Digital de alcance federal integrada por:

a) Autoridad de Aplicación: entre sus funciones está determinar los procedimientos de firma y verificación, conforme estándares tecnológicos internacionales.
b) Comisión Asesora para la Infraestructura de Firma Digital: es una comisión integrada por profesionales de las distintas áreas relacionadas al tema que, entre otras funciones, emite recomendaciones sobre los aspectos técnicos referidos al funcionamiento de la infraestructura de la Firma Digital.
c) Ente Licenciante: la ley de firma digital se refiere en varias ocasiones al Ente Licenciante, aunque el mismo no se encuentra definido en el texto legal. Esta omisión obedece a las modificaciones que el proyecto sufrió a lo largo de su trámite reglamentario, el que eliminó la regulación del ente aunque no todas las referencias al mismo.
   Para suplir la falencia, el decreto reglamentario 2628/02 en su Art. 11 crea el ENTE ADMINISTRADOR de firma digital que es el órgano técnico-administrativo encargado de otorgar las licencias a los certificadores y de supervisar su actividad.

Sin embargo, por el decreto 1028/03 se resolvió disolverlo, trasladando las funciones asignadas a la Oficina Nacional de Tecnologías de Información (ONTI) dependiente de la Subsecretaria de Gestión Pública.

La decisión administrativa 6/2007

El poder ejecutivo mediante la decisión administrativa 6/2007, reglamentó el marco normativo que permitirá la aplicación de la ley 25.506.

Lo importante de esta norma referida al proceso de licenciamiento de certificadores, es que finalmente la Infraestructura de Firma Digital prevista en la Ley 25.506 se encontrará plenamente operativa.

Clase 10 | Comercio Electrónico

El Ministerio de Economía definió al comercio electrónico como "el conjunto de transacciones comerciales y financieras realizadas por medios electrónicos. Esto es el procesamiento y la transmisión electrónica de datos, incluyendo texto, sonido e imagen". En función de la definición se incluirían dentro del concepto no solo las transacciones comerciales sino también cualquier negocio jurídico como la publicidad, edición o cualquier otro servicio.

Contratos Electrónicos

El contrato informático es definido como todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones.

El contrato electrónico se define por los medios utilizados para su realización, la existencia de un intercambio telemático de información durante la celebración o el cumplimiento del contrato.

Según la opinión doctrinaria que elijamos podemos circunscribir el concepto a los contratos celebrados mediante medios informáticos o incluir aquellos en los que el componente electrónico se presenta en cualquier etapa del contrato.

La Ley Modelo sobre Comercio Electrónico dispone que "En la formación de un contrato, de no convenir las partes otra cosa, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos. No se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación un mensaje de datos".

Cabe destacar que no todos los contratos pueden ser celebrados por medios electrónicos, algunos contratos queden excluidos, esto sucedería en los casos que el ordenamiento requiera la existencia de formas solemnes de celebración del negocio jurídico, las que no puedan ser realizadas en forma digital.

Clasificaciones del Contratos Electrónicos

Se clasifican de la siguiente manera:

1. Según los sujetos intervinientes: debe diferenciarse según estemos frente a relaciones que se establezcan con consumidores o entre empresas directamente. Esta es la clasificación más conocida, diferenciando entre comercio electrónico entre empresas (bussines to bussines o B2B) o entre empresas y el consumidor (Bussines to consumer B2C). La presencia de una relación de consumo conlleva la aplicación de los principios

de protección a los particulares establecidos por la legislación de cada país así como por los acuerdos internacionales.

2. Según el tracto contractual: debe separarse aquellas transacciones cuyo cumplimiento se realiza en forma completa por Internet de aquellas en las que alguna de las etapas del contrato debe realizarse en forma tradicional. La obtención de bienes inmateriales como software o simplemente servicios en línea permite la interacción vía web de los contratantes hasta la satisfacción de sus obligaciones, pero otras cosas, como el envío de bienes materiales entre los contratantes, conlleva nuevas relaciones contractuales (contrato de trasporte de mercaderías, seguros, etc.) que exceden al marco de la contratación electrónica.
3. Según la forma de manifestación de la voluntad: debe diferenciarse los métodos que conllevan una simultaneidad en las declaraciones de oferta y aceptación por parte de los contratantes de aquellos en que las manifestaciones se encuentren separadas por un período de tiempo. Esta diferenciación técnica conlleva una consecuencia jurídica importante respecto del momento en el cual se debe considerar realizada tal manifestación.

Competencia Internacional y las cláusulas de prórroga de competencia

El ordenamiento argentino regula el tema de la jurisdicción internacional de los contratos tanto en normas de carácter interno (artículos del código civil) como fuentes del derecho público internacional (tratados y protocolos). Asimismo y en lo referente a operaciones comerciales es posible prorrogar la jurisdicción, salvo que la misma sea exclusiva de la nación argentina o que el pacto de prórroga de competencia se encuentre prohibido.

Es usual incluir dentro de las cláusulas del contrato la prórroga de competencia a favor de un tribunal específico, habitualmente el del domicilio de la parte que estableció los términos del acuerdo. En tal sentido, tanto la jurisprudencia como la doctrina han entendido que en los casos en que la renuncia al fuero establecido por ley implique dejar a la otra parte en un estado de indefensión jurídica, la cláusula es violatoria del principio de defensa en juicio y consecuentemente contraria al orden público argentino.

De no haberse previsto el pacto o en el caso que el mismo sea declarado nulo en sede judicial, el actor puede demandar al deudor en la Argentina en los casos en que este último tuviera domicilio en el territorio o en la hipótesis que el cumplimiento del contrato debería realizarse en la república.

La jurisprudencia ha sido particularmente amplia respecto de habilitar la jurisdicción argentina en contratos internacionales

Ley Aplicable al contrato electrónico internacional

Otro de los problemas que suscita la contratación electrónica es la definición de la legislación aplicable. Para el caso que las partes no hayan establecido convención alguna, el ordenamiento jurídico prevé una serie de normas supletorias de carácter indirecto para determinar el ordenamiento jurídico que regula la situación. En nuestro ordenamiento, el Código Civil establece el principio de la ley del lugar del cumplimiento del contrato. Sin embargo es posible que las características del contrato impliquen la existencia de múltiples lugares ejecución. En tales casos, la jurisprudencia ha entendido que debe utilizarse el lugar de la prestación más característica del contrato en detrimento de las demás.

Para los casos en que no pueda establecerse el lugar de cumplimiento de la prestación, la doctrina entiende que debe aplicarse supletoriamente el art. 1205 del Cod. Civil y utilizarse el lugar de celebración del contrato para definir el régimen aplicable.

Una particularidad del problema se presenta respecto de los contratos que involucran a consumidores, ya que debe tenerse en cuenta la regulación de defensa del consumidor, que no puede ser dejada de lado por medio de convención al contrario.

Es habitual que las empresas que comercian por Internet incluyan este tipo de previsiones, con el fin de limitar los costos judiciales derivados de la comercialización de sus productos. En función de lo analizado, en principio se invalidaría la mayoría de las cláusulas establecidas en lo que respecta a la legislación aplicable a la operatoria.

Sin embargo, la declaración de nulidad de dichos acuerdos implicaría un aumento en los costos de comercialización de las empresas, que deberían conocer la legislación de todos los países donde se sitúen sus clientes.

Atento estas consideraciones, algunos autores han planteado la validez de dichos acuerdos en los casos en que la elección de la normativa aplicable no derive en un abuso de la posición negocial de la empresa.

Otros autores han diferenciado las hipótesis de que se haya realizado comercialización de los productos por parte del proveedor o si simplemente el consumidor accedió a la página por propia iniciativa. Así, Sergio Maldonado sostiene que la directiva europea 97/7/CE habilita la aplicación de la legislación del domicilio del consumidor en los casos en que la empresa haya realizado publicidad en el lugar o mantenido una sucursal en el país. En función de ello, la posibilidad de acceso vía web a los productos no impide la aplicación de las reglas del lugar del establecimiento principal de la empresa.

Para solucionar la falta de seguridad jurídica existente actualmente se está evaluando la conveniencia de suscribir tratados para poder adoptar un criterio uniforme respecto de este tema. Es así como algunos comentaristas han propuesto actualizar la Convención de las Naciones Unidas sobre la Venta Internacional de Bienes para que se incluyan las transacciones de comercio electrónico. En este sentido también la Unión Europea se ha pronunciado sobre la conveniencia de un marco legal único, así como la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional.

La Formación del Contrato

Si la doctrina tradicionalmente ha sostenido que el contrato se perfecciona con la aceptación lisa y llana de una oferta, surge entonces la necesidad de analizar dos cuestiones básicas, la primera, el concepto de oferta en la web, y la segunda, los métodos de manifestación de la voluntad de los contratantes.

El concepto de oferta

La oferta, para ser catalogada como tal, debe ser autosuficiente, conteniendo en su formulación todos los elementos que permitan su aceptación lisa y llana. La oferta a personas indeterminadas no obliga a quien la realiza, constituyendo en realidad una invitación a realizar ofertas por parte de los teóricos aceptantes.

Sin embargo, estos principios se modifican sustancialmente en los casos en que estemos frente a una relación de consumo. En tales casos la oferta se rige por los principios establecidos por la

ley de defensa del consumidor, “la oferta dirigida a consumidores potenciales indeterminados obliga a quien la realiza durante el tiempo en que se realiza, debiendo contener la fecha precisa de comienza y finalización, así como también sus modalidades, condiciones y limitaciones. La revocación de la oferta hecha pública es eficaz una vez que haya sido difundida por medios similares a los empleados para hacerla conocer”. En similar inteligencia, el art. 8 de la ley establece que las precisiones formuladas por la publicidad forman parte de la oferta y resultan obligatorias para el oferente.

Formas de expresión de la aceptación

Debe diferenciarse entre los contratos que se resuelven mediante un formulario incorporado a la propia página, de aquellos en los que el contrato se celebra mediante el intercambio de comunicaciones electrónicas.

En el primero de los casos, existe una forma de interacción instantánea entre los contratantes que impide la existencia de lapso entre oferta y aceptación del contrato. En tales casos no es posible hablar de una retractación sobreviniente de la oferta.

En el caso que el contrato se celebre mediante el intercambio de comunicaciones electrónicas se presenta el problema de determinar en qué momento se debe considerar realizada la aceptación, ya que es posible que el ofertante se retracte en el lapso comprendido entre la manifestación de voluntad del aceptante y su recepción. Dependiendo cuando consideremos realizada la aceptación, el contrato ya se habría celebrado (o no) y por tanto, la retractación podría devenir en invalida.

Expresión de la voluntad mediante formularios Web: Clic and Warp Agreement y Browse Agreement

En ambos casos nos encontramos con contratos de adhesión realizados mediante un formulario incluido dentro de la programación de la página, de forma tal que el acuerdo se celebrar íntegramente mediante esta.

Los clic and warp agreements es la denominación del acuerdo en que la aceptación se realiza mediante un cuadro de dialogo ofrecido por el programa donde el usuario interacciona con el mouse sobre una interfaz prefijada (normalmente un botón de aceptar o declinar) para manifestar su voluntad. Esta ventana impide el acceso a la prestación, funcionando como una barrera hasta que el usuario acepte los términos del contrato. En forma general, la validez de los click agreement está supeditada al real conocimiento por parte del usuario del contenido del contrato.

En los browse agreement en cambio no es necesario manifestar la voluntad en forma expresa: La utilización de los servicios del sitio web hacen presumir la conformidad de los términos y condiciones de la página por parte de los usuarios, los que quedan contractualmente obligados en los términos establecidos de antemano.

Usualmente, las condiciones de contratación se encuentran incluidos mediante un hipervínculo colocado al final de la página, bajo la denominación “legales” o simplemente “términos y condiciones”. Atento ello, los usuarios pueden utilizar los servicios del sitio o descargar sus productos sin acceder a los mismos ni conocerlos.

La legalidad de dichos acuerdos es objeto de debate. La corte sostuvo que el inicio de la descarga del producto, y en realidad cualquier otra actividad en la web, no tiene como objeto

la manifestación de voluntad sino la obtención de un bien inmaterial. La inexistencia de un cuadro de dialogo que permita expresar llanamente la conformidad con el contrato previamente expuesto impide considerar que se ha celebrado una convención.

Debe tenerse en cuenta que la validez del acuerdo browse se haya supeditada a la existencia de un aviso claro por parte de proveedor de servicios informáticos respecto a la existencia de las condiciones de contratación. Se genera la necesidad de asegurar la facilidad de acceso del usuario a los mismos, evitando que la utilización de términos o gráficos que lo oculten o dificulten su lectura. En el mismo sentido, los términos deben encontrarse en la página principal del sitio o por lo menos en la página de acceso al mismo.

Contratos Celebrados mediante comunicaciones electrónicas

A diferencia de los contratos celebrados directamente sobre la página web, las convenciones realizadas mediante comunicaciones electrónicas plantean un lapso entre la expresión de la declaración de voluntad aceptando la oferta y la actual recepción por parte del ofertante. En tal sentido, estos acuerdos mantienen todas las características de los tradicionales contratos entre ausentes (distancia geográfica/temporal), pudiendo por tanto aplicar las soluciones establecidas para dicho instituto.

El principal problema es la definición del momento en que se da por formado el consentimiento, variando las soluciones según el ordenamiento que se tome en consideración. Las principales teorías son las siguientes:

1. Teoría de la expresión de la voluntad: el consentimiento se da por realizado con la mera expresión de la voluntad, con prescindencia de la comunicación al ofertante.
2. Teoría de la cognición: la voluntad se da por formada con el conocimiento de la otra parte. Esta es la solución adoptada por la mayoría de las legislaciones del derecho continental europeo.
3. Teoría de la recepción: la voluntad se da por formada con la recepción de la manifestación de la voluntad por parte del ofertante.
4. Teoría de la emisión: la voluntad se da por constituida cuando el aceptante envía la notificación a la contraparte, con prescindencia de la actual recepción.

El ordenamiento argentino usa esta última doctrina. Excepcionalmente, el código civil prevé la utilización de la teoría del conocimiento en dos casos, el art. 1155, que prevé la posibilidad de retractar la aceptación antes de que la misma llegue a conocimiento del ofertante, y el art. 1149, que dicta que en los casos de incapacidad o muerte sobreviniente del proponente, el contrato se considerará celebrado en los casos en que el ofertante tuvo conocimiento de la aceptación y no cuando esta se envió.

Asimismo debe tenerse en cuenta que en las hipótesis de relaciones de consumo, la ley de defensa al consumidor, otorga al consumidor el derecho a revocar la aceptación durante el plazo de 5 días de recibida la cosa adquirida por medios telefónicos o postales. Esta solución tiene su fundamento en la necesidad de evaluar las características reales del producto y no puede ser renunciada.

Medios de Pago Electrónicos

La denominación medios de pago electrónicos engloba a los medios de satisfacer las obligaciones que utilicen total o parcialmente una red de computadores para su realización.

Actualmente existen empresas que brindan soluciones de intermediación financiera para realizar las compras por Internet. Asimismo, ha surgido el llamado “dinero electrónico”, sistema que acredita un crédito mediante el depósito por anticipado de sumas de dinero que queda disponible en un dispositivo que queda en poder del depositario.

La utilización de tarjetas de crédito presenta dos problemas fundamentales. El primero es considerar cuando se produjo el pago en sí mismo, mientras que el segundo deriva de la necesidad de asegurar las transacciones realizadas.

Para entender el problema de la acreditación del pago, es necesario observar que en realidad existen dos obligaciones diversas. Una vez acreditada la operación entre el cliente y el sitio de Internet, surge en la entidad de crédito la obligación de abonar las sumas presentadas al cobro, toda vez que se ha obligado a cubrir las dichas deudas mediante el contrato de tarjeta de crédito. Sin embargo, al mismo tiempo nace la obligación del cliente de abonar las sumas pagadas y acreditadas en su resumen. Se trata en suma de dos obligaciones independientes.

Respecto a asegurar las transacciones, siempre existe el riesgo de que se imputen al titular de la tarjeta operaciones que no realizadas. En tal caso, la ley de tarjetas de crédito permite la impugnación del saldo de tarjeta en un plazo de 30 días desde que fue recibido. El emisor en tal caso debe acusar recibo de la impugnación dentro de los siete días siguientes y presentar los comprobantes o fundamentos del débito en el lapso de 15. En el caso de operaciones realizadas por Internet se presenta el problema de la ausencia de comprobantes firmados por el titular, lo que dificultaría la prueba.

Respecto a la seguridad, actualmente existen varios sistemas de seguridad destinados a encriptar las comunicaciones y resguardar los datos financieros de los titulares de la tarjeta. Los dos principales son el SSL (secure socket layer) desarrollado por Netscape y el SET creado por las empresas Visa y MasterCard.

El SSL no es, en realidad, un sistema de pago sino un mecanismo de carácter general destinado a asegurar las comunicaciones realizadas vía web. Si bien es el más sencillo, presenta algunas objeciones al momento de su aplicación. En primer lugar, la conexión segura se establece entre los contratantes solamente dejando de lado al intermediario financiero. En segundo, trasmite los datos sin corroborar al comerciante, solución que permite el abuso por parte de una parte inescrupulosa ya el sitio sea perjudicado con la presentación de una tarjeta fraudulenta o que se carguen consumos en detrimento del titular de la misma.

El SET, en cambio, constituye un protocolo destinado específicamente al comercio electrónico, incorporando a todos los sujetos de la transacción. De la misma forma elimina muchas de las inseguridades de la transacción, ya que evita que el comerciante conozca los datos de la tarjeta, al mismo tiempo que impide a la entidad financiera conocer los consumos realzados. El mayor problema para la adopción de este sistema es que resulta engorroso tanto para el usuario como para el sitio web, siendo necesaria la inversión en software y equipos, los cuales muchas veces no son compatibles entre sí.

Asimismo es posible la utilización de intermediarios financieros, siendo quizás el más conocido PayPal. La operatoria en tales casos necesita que el cliente ingrese en el sitio del intermediario la información de su tarjeta, siéndole entregado un número de identificación para realizar las transacciones en los sitios adheridos. Estos, a su vez, acreditan la compra con el intermediario, quien procede a imputar el débito en la tarjeta del usuario.

Este sistema soluciona parcialmente el problema de la seguridad, evitando tener que ingresar la información en cada una de las operaciones. Sin embargo, no evita la posibilidad de ataques a las bases del intermediario, que sigue manteniendo la información sensible.

Por último, otro sistema posible es el llamado dinero digital. Tal como ya analizáramos en tales casos, el cliente deposita, adquiere o consigna los valores recibiendo a cambio una tarjeta inteligente o una clave donde se registran los valores disponibles.

Clase ¿ | Comentarios del Fallo Belén Rodríguez (lo dejo porque está bueno para leerlo por encima)

La responsabilidad de los buscadores de Internet después del caso Belén Rodríguez

El fallo de Corte de "Belen Rodriguez c/ Google inc s/Daños y perjucios" pone fin a una discusión respecto a la responsabilidad de los buscadores de internet por el contenido indexado por el servicio, cuando el mismo produce un daño indemnizable.

La cuestión en debate es si los buscadores pueden ser responsabilizados por hechos de los cuales no son autores y en caso afirmativo, cual es el factor de imputación. La postura negativa fundamenta la idea en la ausencia de autoría, sosteniendo que los buscadores carecen de control editorial sobre los contenidos que indexan, transformándose más en el equivalente a una biblioteca que a una editorial. En contraposición, los autores que sostienen una postura cercana a la responsabilidad refieren que los demandados no son otra cosa que una empresa que presta de un servicio, obteniendo un beneficio económico de las búsquedas realizadas, por lo que deben ser responsabilizados cuando estos resultados producen un resultado dañoso.

La falta de responsabilidad de los buscadores implicaría una ausencia de reparación de los damnificados, que deberían cargar con las consecuencias de los actos ilícitos.

Al mismo tiempo, la responsabilidad de los navegadores tiene una incidencia directa sobre la libertad de expresión. Es una consecuencia lógica de la responsabilidad la capacidad de control de las empresas en cuanto a los contenidos a indexar, abriendo la posibilidad de censura de contenidos o la desaparición de enlaces objetables.

Por todo lo expuesto cualquier solución a adoptar debe necesariamente realizar un compromiso entre estos dos valores jurídicos (defensa efectiva de la privacidad y libertad de expresión) estableciendo los mecanismos para determinar en qué casos y bajo qué condiciones, un valor jurídico básico de como la libertad de expresión puede ser limitado.

En la República Argentina no existe una legislación específica que regule el tema de la responsabilidad civil de los prestadores de servicios de información. Atento ello, la discusión ha pasado en forma casi exclusiva por la doctrina y la jurisprudencia, a lo que debe sumarse algún proyecto legislativo que intentaba reglamentar la cuestión.

Dentro del campo de la doctrina, podemos dividir a los autores entre los que consideran un factor de imputación objetivo, basado en el riesgo creado, de aquellos que sostienen una responsabilidad de carácter subjetiva, basada en la negligencia en el control o accionar del buscador.

Dentro de los autores que sostienen un reclamo con base en la culpa de los buscadores debe separarse a aquellos que sostienen los buscadores comienzan a ser responsables después

recibida la orden de autoridad competente, de aquellos que sostienen que la obligación de actuar comienza en el momento en que reciben la noticia del ilícito, sea que esta provenga de una notificación judicial o simplemente de un tercero.

La posición de aquellos que sostienen la mera noticia como disparador de la responsabilidad se fundamenta en el hecho que el buscador, como todo hombre de negocios, debe actuar con buena fe y diligencia ante la noticia de un ilícito manifiesto, según el principio básico de no dañar al otro.

El caso Belén Rodríguez. Antecedentes

En el proceso se discute la responsabilidad de los buscadores de Internet por la invasión a la privacidad de un particular, la actora Belen Rodriguez, de profesión modelo, quien manifiesta que los resultados de búsqueda obtenidos por los demandados la vinculan a sitios de contenido sexual. Al mismo tiempo, se plantea una violación a su derecho a la imagen en cuanto a la utilización, por parte del buscador, de fotografías sin autorización publicadas por terceras partes, las que, reducidas en tamaño y resolución, son presentadas como resultado de la referida búsqueda bajo el nombre de thumbnails.

El fallo de primera instancia condena a los buscadores a una indemnización monetaria por entender que existe un accionar negligente. Si bien rechaza la idea de una responsabilidad objetiva, entiende que la omisión de evitar el daño por parte de las demandadas a pesar de estar fehacientemente notificadas por la realización de la audiencia de conciliación, así como de la formación del incidente de cautelar, permiten imputar una responsabilidad. En tal sentido ha sostenido que “Si bien dichas empresas son proveedoras de herramientas de búsqueda -no de contenidos- advertidas por la afectada (…) debieron sin demora proceder a impedir o bloquear cualquier tipo de acceso a los contenidos cuestionados”. Se lo considera una negligencia culpable.

Debe tenerse en cuenta que en el fallo de primera instancia el accionar de los buscadores debía satisfacer una pretensión de carácter difuso, como es bloquear todas las entradas que violen los derechos de la demandada y no solo aquellas que fueron denunciadas por la misma. De esta forma el fallo de primera instancia establece en el punto II de la sentencia que “...Dispongo la eliminación definitiva de las vinculaciones del nombre, imagen, y fotografías de la actora con sitios y actividades de contenido sexual, erótico y/o pornográfico a través de los buscadores www.google.com.ar y www. yahoo.com.ar”.

Sin embargo, el fallo de cámara revierte parcialmente lo establecido en primera instancia, limita la responsabilidad a los casos denunciados por la actora, rechazando la pretensión de una cautelar genérica. Esta cuestión se relaciona con la discusión acerca de si basta con un pedido genérico (de retiro de todos los contenidos, cualquiera sea el sitio en el que se encuentren, que resulten perjudiciales para el peticionante), o si debe señalarse cada sitio web en particular.

La pericia deja en claro que los eventuales filtros que puedan emplearse trabajan sobre palabras; lo que puede “bloquearse”, entonces, es la asociación de ciertos términos con otros...” “...la exclusión de determinadas palabras puede pecar por exceso (por ejemplo, eliminando también el acceso a páginas referidas a homónimos) o por defecto (porque pueden quedar fuera otros contenidos agraviantes en los que se expresen similares conceptos mediante el empleo de palabras distintas)”... “No puede admitirse, entonces, en principio, un

pedido genérico de detección y retiro de ciertos contenidos, cualquiera sea el sitio en el que se encuentren".

Atento que ambos buscadores al ser notificados habían procedido a bloquear las direcciones denunciadas por la actora, el fallo rechaza la posibilidad de una indemnización. Sin embargo, y respecto de Google en particular, la existencia de los thumbnails se vuelve fuente de responsabilidad civil.

Según la interpretación del fallo, la generación de estas imágenes implica su apropiación por parte del Google, quien las incorpora dentro de su página como un elemento apreciable para los terceros. Resulta claro para el sentenciante que la empresa habría excedido el mero papel de indexador, reproduciendo sin autorización la imagen de la actora.

"Google ha utilizado y reproducido imágenes de la actora -reduciéndolas, almacenándolas, y publicándolas en su buscador de imágenes- sin su consentimiento, lo cual, en ausencia de un régimen especial que establezca una excepción para estos casos, resulta violatorio de lo prescripto por el art. 31 de la ley 11.723".

Por todo lo expuesto, el fallo de cámara modifica parcialmente el de primera instancia condenando a Google a indemnizar la apropiación de las imágenes y rechazando la demanda contra el buscador Yahoo.com.

El fallo de Corte. Análisis del voto mayoritario y su disidencia.

La Corte Suprema resolvió finalmente el caso. Sin embargo, no fue un fallo unánime, teniendo una disidencia parcial de los doctores Lorenzetti y Maqueda que resulta necesario analizar atento su importancia.

El fallo de mayoría rechaza la responsabilidad objetiva como factor de imputación, estableciendo un criterio subjetivo de base constitucional.

En este sentido el fallo relaciona la responsabilidad de los buscadores en forma directa con la libertad de expresión. De tal forma, los buscadores cumplen una función esencial al permitir la libre circulación de las ideas, principio consagrado en nuestra carta magna, por lo que toda interpretación que se haga desde el derecho civil debe necesariamente armonizar con los principios constitucionales.

Por tanto la sanción de una responsabilidad objetiva implicaría una limitación injustificable accionar de un tercero que, en principio, no ha tenido control editorial sobre los contenidos dañosos, con la consiguiente disminución en una actividad, en principio lícita.

La Corte ha sostenido que "que responsabilizar a los "buscadores" -como principio- por contenidos que no han creado, equivaldría a sancionar a la biblioteca que, a través de sus ficheros y catálogos, ha permitido la localización de un libro de contenido dañino, so pretexto que habría "facilitado" el daño. Más allá de que la sanción sería injusta, es muy probable que -de seguirse ese criterio "objetivo" de responsabilidad- terminarán cerrándose muchas bibliotecas, con gran perjuicio de los lectores".

Si el Superior Tribunal sitúa la responsabilidad dentro del campo de la culpa cabe determinar cuál es su conducta debida, establecer en qué momento comienza la obligación de bloquear los contenidos ilícitos y cuál es la extensión de ese bloqueo.

Respecto a la primera cuestión, el fallo diferencia entre aquellos contenidos manifiestamente ilícitos de aquellos donde sea necesaria la determinación judicial, obligando en el primer caso a

bloquear los contenidos con la mera notificación extrajudicial, mientras que en el segundo se requerirá una orden judicial competente.

Este sistema, si bien resulta la solución de compromiso que quizás más acerque a compatibilizar el principio de libertad de expresión con la necesidad de resguardar a los particulares, se aparta de la mayoría de los sistemas adoptados en la legislación comparada.

Un segundo problema respecto a la solución adoptada es el contenido de cada una de las categorías, es decir en qué casos nos encontramos frente a un contenido manifiesta y groseramente ilícito. La propia corte realiza una enunciación pero el contenido mismo de los hechos listados puede ser sujeto a debate. Así, el listado refiere a datos que "faciliten la comisión de delitos, que instruyan acerca de estos, que pongan en peligro la vida o la integridad física de alguna o muchas personas". Con estas reglas, por ejemplo, la información referente a DRM y hacking estaría en debate, los DRM no han sido declarados ilícitos por la mayoría de las legislaciones y en cuanto al hacking debe tenerse en cuenta que no todo acceso forzoso es ilícito sino solo aquel que se realiza sin autorización o excediendo la prestada, por lo la información técnica no puede ser catalogada per se cómo ilícita, bajo el riesgo, en un futuro próximo, de censurar toda información sobre cerrajería atento su posible utilización en un robo.

Respecto al extensión del bloqueo, el voto mayoritario adhiere al criterio de cámara en cuanto a la necesidad de individualización de los contenidos a bloquear. Pero mientras el fallo de cámara tenía un fundamento eminentemente técnico en base a la imposibilidad de filtrar correctamente a los resultados de homónimos, el fallo de corte suma una argumentación jurídica, el fallo juzgó que la aplicación de filtros implica una tutela preventiva a contenidos por suceder que comporta una restricción a la libertad de expresión.

Por último y respecto a la responsabilidad derivada de los llamados thumbnails, la corte rechaza el fallo de Cámara por entender que los mismos consisten solamente en una referencia del contenido generado por una tercera persona, por lo que no existe base para establecer un régimen legal diferente al utilizado para los aquellos contenidos expresados mediante texto.

Este criterio, junto con la posibilidad de establecer medidas precautorias son el fundamento de la disidencia parcial de los doctores Lorenzetti y Maqueda. En el primero de los temas, sostienen el criterio de Cámara respecto a la responsabilidad de los buscadores por los thumbnails entendiendo que la creación de los mismos constituye una apropiación sin autorización, la cual puede ser accedida por usuario.

En opinión del autor de la presente, el mero fundamento técnico no aparece como suficiente para establecer un tratamiento diferenciado de los contenidos de texto. Mas teniendo en cuenta que estos últimos también son almacenados en forma automatizada por los crawlers de Google, la cual es accesible cuando la página original se encuentra indisponible. Por ende, aparece como un contrasentido frente a una ilicitud declarar la responsabilidad de un caso y eximirla en el otro cuando en ambos casos se ha generado una copia a los efectos de referencia.

Respecto a la posibilidad de una protección preventiva el fallo minoritario establece su procedencia, entendiendo que, en base a la obligación de evitar el daño, los buscadores deberían arbitrar los medios para filtrar aquellos contenidos. En tal sentido, "...mediante esta vía resulta posible que una vez corroborada la existencia de vinculaciones que claramente

lesionan derechos personalísimos de una persona, esta pueda requerir judicialmente a los "motores de búsqueda" que, acorde con la tecnología disponible, adopten las medidas necesarias tanto para suprimir la vinculación del damnificado con enlaces existentes de idénticas características como para evitar que en el futuro se establezcan nuevos vínculos de igual tipo…"

Consideraciones finales

El fallo en el caso Rodríguez significó adoptar para el derecho interno un estándar compartido por la mayoría de la doctrina y legislación comparada al mismo tiempo que criterio de resolución de los numerosos casos que se encontraban pendientes.

Sin embargo en opinión de autor de la presente, existen cuestiones que todavía serán objeto de debates. En primer término, el ya mencionado estándar de "ilicitud manifiesta y grosera" es posible que sea fuente de litigio en aquellos casos en que esta calidad no sea palmaria, excepto en la hipótesis que, con el fin de evitar costos judiciales, los buscadores adopten una interpretación amplia de la figura y voluntariamente bloqueen los contenidos observados por los particulares.

En segundo lugar, el fallo no menciona nada respecto del derecho al olvido (posibilidad de dar de baja o desindexar cierta información), esta ausencia no ha pasado desapercibida para la doctrina y constituye un tema a debatir en el futuro.

Por último, el autor no puede dejar de señalar que la propia dinámica de los miembros de la corte puede llevar a la variación de los criterios del fallo mayoritario. Atento la jubilación del Dr. Zaffaronni y la avanzada edad del Dr. Fayt, es posible que pronto los autores de la disidencia se encuentren en condiciones de constituirse en una nueva mayoría, lo que puede variar los criterios expuestos, en particular respecto de la posibilidad de cautelares o sentencias que orden un bloqueo genérico o preventivo de los elementos ilícitos.

Clase 11 | Proyecto sobre delitos informáticos

Introducción

El proyecto que analizaremos posee el consenso en sus principales aspectos de gran parte de la industria, de especialistas, de académicos y ha recibido el respaldo de ambas cámaras del Congreso. Por eso es prometedor que se avecine la posibilidad de que el Código Penal argentino finalmente contemple delitos relacionados con Internet y las nuevas tecnologías.

La mayoría de los códigos penales modernos del mundo han contemplado alguna forma de criminalidad relacionada con la informática, hasta existe una convención internacional sobre la materia, el delito informático ya no puede ser ignorado por el legislador.

A fines del año 2006 la cámara de diputados aprobó el proyecto de ley. El proyecto contempló los delitos informáticos más tradicionales tales como la estafa informática, el daño informático, el acceso no autorizado a un ordenador, la falsificación de documentos digitales, y la violación de correspondencia digital, correo electrónico y cualquier otro medio de comunicación moderno así como su interrupción. También se contemplan delitos relacionados con la pedofilia y la distribución de virus informáticos.

Durante el año 2007 el Senado aprobó con reformas el proyecto. Se trata de una reforma al Código Penal, no de una ley de delitos informáticos. Por eso en líneas generales no se crean

nuevos delitos sino que se modifican ciertos aspectos de los existentes para receptar las nuevas tecnologías.

Análisis del proyecto de reforma

Definiciones

La primera reforma propone incorporar al artículo 77 del Código Penal las siguientes definiciones:

- El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.
- Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente.
- Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.

El nuevo delito de ofrecimiento y distribución de imágenes relacionadas con la pornografía infantil

En nuestro país la ley 25.763 aprobó el Protocolo relativo a la venta de niños, la prostitución infantil y la utilización de los niños en la pornografía, que complementa la Convención de las Naciones Unidas sobre los Derechos del Niño. El artículo 1 de dicho Protocolo dispone que "Los Estados Parte prohibirán la venta de niños, la prostitución infantil y *la pornografía infantil".*

Por "pornografía infantil" se entiende toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales (art. 2).

El art. 3 dispone que "Todo Estado Parte adoptará medidas para que, como mínimo, los actos y actividades que a continuación se enumeran queden íntegramente comprendidos en su legislación penal, tanto si se han cometido dentro como fuera de sus fronteras, o si se han perpetrado individual o colectivamente:

- La producción, distribución, divulgación, importación, exportación, oferta, venta o posesión, con los fines antes señalados, de pornografía infantil, en el sentido en que se define en el artículo 2.
- Entre otros

El proyecto propone sustituir el artículo 128 del Código Penal, por el siguiente: "Artículo 128.- Será reprimido con prisión de seis meses a cuatro años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores. Será reprimido con prisión de cuatro meses a dos años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización. Será reprimido con prisión de un mes a tres años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce años."

Esta versión del Senado es similar a la redactada inicialmente en la cámara de diputados. Pero el dictamen del Senado sustituyó imágenes pornográficas por "toda representación". Hay que notar que en ninguna de las versiones finales de ambas Cámaras se incluyó la mención de actividades sexuales simuladas, la idea circuló en el Senado pero por considerárselo controvertido tampoco se lo incluyó pese a que lo prevé el Protocolo Facultativo de la Convención sobre los Derechos del Niño y la Convención del Ciberdelito.

En la cámara de Diputados la reforma del art. 128 del CP había dejado de lado –por un error involuntario- la figura del que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren menores. La nueva redacción del Senado reinstala tal delito.

en relación al proyecto de Diputados el Senado alteró las penas que el proyecto prevé para la producción y la tenencia y se agregó un requisito más a la tenencia para penalizar sólo aquella que tenga fines inequívocos de comercialización o distribución. El dictamen del Senado (OD 959/2007) explica así estos cambios *"No se consideró conveniente reprimir con la misma pena a quién distribuya representaciones de las descriptas en el párrafo anterior como a quien las tenga en su poder, ya que son ilícitos de diferente peligrosidad"*.

Esta nueva figura generó preocupación en las empresas que actúan como intermediarios en Internet (tales como empresas de telecomunicaciones, ISP, hosting, etc.), quienes consideraron que podría llegar a imputárseles responsabilidad penal por los contenidos que transitan o se albergan (en el caso de hosting) en sus servidores, pese a que usualmente no tienen conocimiento acabado de la ilicitud del contenido en cuestión.

Pero, en estos casos, no es posible inferir que se incurra en el delito. Para ello nos basamos en lo siguiente:

1. No existe conocimiento efectivo de los contenidos y de su ilicitud;
2. En la mayoría de los casos no podría existir tal conocimiento por la inviolabilidad de las comunicaciones;
3. Sumado a la inexistencia de un deber de vigilancia o supervisión de contenidos.

En todo el derecho comparado se considera a ésta como una figura dolosa (que si tiene conocimiento del ilícito).

Para los usuarios que poseen en sus discos una imagen sin conocimiento de dicha posesión, nuevamente, la falta de dolo hace que no exista delito. Tal supuesto se daría en el caso de un usuario que "baja" directamente de Internet (o a través de una red peer to peer) un archivo zipeado sin conocer su contenido en el entendimiento que es una película o archivo musical según el título del archivo, pero que luego resulta que contiene imágenes prohibidas por el art. 128 CP. EN este caso entendemos que tampoco habría presencia de la finalidad de distribuir o comercializar que exige el segundo párrafo del art. 128 CP.

También podría darse el supuesto de un usuario adulto que solamente visualiza esas imágenes online (acción que el art 128 CP no prohíbe) sin grabarlas, pero que por la configuración técnica del ordenador quedan grabadas en la memoria cache del navegador sin su consentimiento. La jurisprudencia norteamericana sostuvo que no se daban los elementos del tipo penal de tenencia de imágenes de pornografía infantil. A similares conclusiones llegó la doctrina.

Violación de Secretos y de la Privacidad

a) Nuevo epígrafe para el Código Penal: el derecho a la privacidad

La reforma del Senado conservó la propuesta de la Cámara de Diputados de incluir a la "privacidad" como bien jurídico protegido. Explica el dictamen del Senado que "sobre todo a tenor de lo prescripto por el inciso 3 del artículo 157 ("3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales"), ya que la norma se entiende más como afectación a la intimidad que al bien jurídico secreto". El art. 153 bis propuesto también refuerza la protección de este bien jurídico en ambientes digitales.

El bien jurídico penalmente protegido es el determinado previamente como tal por una comunidad ubicada en el tiempo y en el espacio, que, por decirlo de alguna manera, elige qué entidad merece ser considerada como bien por satisfacer sus necesidades individuales y sociales. No cabe duda que las nuevas tecnologías han aumentado los riesgos y peligros para el derecho a la privacidad. Hoy en día existen cientos de bases de datos con nuestros datos personales, y constantemente nos encontramos con nuevos casos de robo de identidad, sustracción de información personal o venta masiva de bases de datos personales.

Ante todo este panorama, el derecho penal debe acompañar estos cambios con nuevas normas que se adecuen a la realidad tecnológica actual pero también con nuevos bienes jurídicos que conceptualicen esas necesidades.

b) Violación de correspondencia digital

El proyecto sustituye el artículo 153 del Código Penal, por el siguiente: "Artículo 153.- Será reprimido con prisión de quince días a seis meses el que abriere o accediere indebidamente a *una comunicación electrónica*, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de *una comunicación electrónica*, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o *una comunicación electrónica* que no le esté dirigida".

Se agrega asimismo un párrafo que dispone "En la misma pena incurrirá el que *indebidamente* interceptare o captare *comunicaciones electrónicas o telecomunicaciones* provenientes de cualquier sistema de carácter privado o de acceso restringido".

Tal como actualmente reza el actual artículo 153 se prevé que "La pena será de prisión de un mes a un año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica" (se reemplaza culpable por autor y se agrega la mención de "comunicación electrónica").

Se agrega además que "Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.".

Salvo por lo dispuesto en este último párrafo, el proyecto que comentamos no innova creando nuevos tipos penales, sino que a los existentes les agrega el término "comunicación electrónica" para actualizarlos.

En la redacción final la palabra "indebidamente" aparece repetida. En este caso, como en otros, la expresión (indebida) tiene el sentido de fundar el delito sobre una firme y delineada

figura objetiva y subjetiva de licitud que excluye toda posibilidad de imputar el delito en forma culposa". Es decir, esta figura sigue siendo un delito doloso.

Con esta aclaración quedan salvadas las objeciones de ciertos medios empresarios que abrigaban el temor que esta figura penal fuera aplicada a acciones de un proveedor de acceso a Internet o de servicios de mail tales como desviar un correo electrónico porque contiene un virus o porque un algoritmo o filtro lo clasifica como spam. No es la finalidad de la nueva figura prevista en el art. 153 del CP el penalizar tales situaciones. Pero además nunca podría llegarse a tal resultado interpretativo por la carencia de dolo en tal accionar. Asimismo cabe resaltar que el término "indebido" es también sinónimo de realizado sin derecho. En tal sentido, un ISP o proveedor de servicio de correo, está en su derecho, según sus términos y condiciones de uso, de desviar o etiquetar correspondencia no solicitada (spam) que es ilegal en Argentina, o de suprimir aquella que constituya una amenaza para su seguridad o la de sus usuarios si contiene virus o algún programa potencialmente dañino.

Ello se ve corroborado por el dictamen del Senado (OD 959/2007) que fundamenta "es razonable la propuesta de incorporar no sólo la comunicación electrónica sino también la expresión "indebidamente", para que no le queden dudas al intérprete respecto a requerir la finalidad dolosa del autor del delito, y evitar cualquier hermenéutica tendiente a considerar comprendidos en el tipo a quienes en procura de mejorar el servicio que prestan a sus usuarios, activan mecanismos de protección para evitar lo que se conoce como spam, o la recepción de correos no deseados por sus clientes".

c) Acceso ilegítimo a un sistema informático

La reforma incorpora como art. 153 bis del Código Penal, el siguiente: "Artículo 153 bis. Será reprimido con prisión de quince días a seis meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido. La pena será de un mes a un año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros."

Cabe señalar que son numerosas las jurisdicciones que penalizan el acceso ilegítimo a sistemas informáticos pues estos suelen ser la antesala para la comisión de otros delitos como la estafa, el daño, la sustracción de datos personales, de claves o de secretos comerciales. En esa inteligencia, el legislador estableció que solo resultará de aplicación esta figura "si no resultare un delito más severamente penado".

El texto legal hace referencia a "sistema o dato informático de acceso restringido" puesto que no se prohíbe acceder a sistemas o redes abiertas, o al contenido publicado en un sitio de Internet público (como son la gran mayoría).

Esta disposición causó inicialmente alarma en más de un programador que consideró que la norma en cuestión podría aplicarse al ethical hacking, pero en la práctica, si ocurre con consentimiento del dueño o titular de la red que está siendo testeada, existe una autorización legal por parte de la "víctima", con lo cual no se da el elemento del tipo que requiere que el acceso ocurra "sin la debida autorización o excediendo la que posea". Esta autorización puede

tomar cualquier forma, pero generalmente se verá reflejada en un contrato de servicios de seguridad informática.

Cabe aclarar también que esta figura no está destinada a prohibir la ingeniería inversa (o ingeniería reversa). El objetivo de la ingeniería inversa es obtener información técnica a partir de un producto accesible al público, con el fin de determinar de qué está hecho, qué lo hace funcionar y cómo fue fabricado. Los productos más comunes que son sometidos a la ingeniería inversa son los programas de computadoras y los componentes electrónicos. Por ejemplo un usuario legítimo puede abrir un programa informático con el fin de corregirle un error o permitir que corra en otro sistema operativo, o abrir un contenido (ej. un DVD) para poder leerlo en otra plataforma si está encriptado originariamente, o en la consola de la competencia, o "abrir" un teléfono celular para poder hacerlo funcionar en otro proveedor distinto o abrir una rutina de filtrado de contenidos en Internet para averiguar que sitios filtra y "si filtra de más o de menos" sitios inocentes. El listado de acciones es interminable.

Como es dable observar, todas de esas situaciones están relacionadas con la protección de la propiedad intelectual (tales como el derecho de autor o patentes, que este proyecto no tratan), mientras que el bien jurídico protegido por la figura que estudiamos (art. 153 bis del CP) es la privacidad. Por ende, partiendo del objeto de la protección penal, está claro que cualquier intento de utilizar esta figura para frenar un acto de ingeniería inversa no debería tener recepción judicial. De hecho la ley de patentes contiene excepciones para experimentación antes del vencimiento de la misma.

Lo relativo a las medidas de protección tecnológica, que limitan en cierto modo la ingeniería inversa, fue introducido en el Tratado de Derecho de Autor de la OMPI del año 1996, que nuestro país aprobó oportunamente, pero que todavía no reglamentó ni en el ámbito civil ni en el ámbito penal.

La Corte Suprema fue muy clara en cuanto a que un tratado internacional no alcanza para crear un delito, y que para que haya delito se requiere una ley del Congreso. Al no haber ley del Congreso que en forma específica sancione penalmente la ingeniería inversa (lo cual podría considerarse una pésima decisión de política legislativa), mal podría aplicarse el tipo penal del art. 153 bis del CP a estos casos.

d) Publicación abusiva de correspondencia

Se actualiza el art. 155 siguiendo la misma técnica del art. 153 reformado (agregado del término *comunicación electrónica*). La nueva redacción del artículo 155 del Código Penal reprime con multa al "que hallándose en posesión de una correspondencia, *una comunicación electrónica*, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere *publicar* indebidamente, si el hecho causare o pudiere causar perjuicios a terceros".

Cabe preguntarse si seguirá vigente aquello que la doctrina señalaba respecto a que, en esta figura, el concepto de publicar una cosa es ponerla al alcance de un número indeterminado de personas, pero la comunicación privada y personal, aunque sea a un cierto número de personas no es suficiente.

Se agrega la disposición que no se encuentra en el actual art. 155 del CP y que reza: "Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de

proteger un interés público". La norma, reproduciendo claramente la idea subyacente en el art. 111 inc. 1 del CP para las calumnias, busca eximir de responsabilidad penal a quien revela una correspondencia cuyo contenido es de claro interés público.

e) Revelación de secretos

Se sustituye el artículo 157 del Código Penal, por el siguiente texto: "Será reprimido con prisión de un mes a dos años e inhabilitación especial de uno a cuatro años, el funcionario público que revelare hechos, actuaciones, documentos o *datos*, que por ley deben ser secretos.". Se agrega el término datos para actualizar esta figura.

f) Unificación de los tipos penales de los arts. 117 bis y 157 bis del CP: acceso a un banco de datos, revelación de información y alteración de datos

El proyecto de reforma modifica el artículo 157 bis del Código Penal, por el siguiente:

"Artículo 157 Bis.- Será reprimido con la pena de prisión de un mes a dos años el que:

> 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;
>
> 2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.
>
> 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años."

El Senado consideró de adecuada técnica legislativa unificar los artículos 9 y 10 del proyecto de Diputados (que establecían los delitos de insertar datos falsos y revelar información de un banco de datos respectivamente) en una sola norma, ya que ambos refieren a modificaciones del artículo 157 bis Código Penal.

Al unificar las normas del art. 117 bis y del art. 157 bis CP en una sola además se propone derogar el art. 117 bis, para no incurrir en redundancias.

Hay que resaltar que estos tipos penales introducidos por la ley 25.326 de protección de datos no fueron muy eficaces y están sujetos a controversias de diversa clase. Sin entrar en profundidad nunca se aclaró si eran delitos de acción pública o de acción privada.

g) Captación ilegal de datos, imágenes y sonidos

La norma contenida en el artículo 6° del proyecto aprobado por la Cámara de Diputados establecía en forma muy amplia un delito que consistía en la obtención o captación de la imagen, sonidos o datos de una persona en forma ilegal y su posterior difusión. El Senado prefirió no incluir este delito en el proyecto.

El dictamen del Senado (OD 959/2007) explica así esta eliminación: "La norma contenida en el artículo 6° del proyecto aprobado por la Cámara de origen fue cuestionada, porque se infiere

de la misma la punición de las cámaras ocultas, lo que se consideró merecedor de otro debate en cuanto no se encuentra directamente vinculado a la materia de esta iniciativa: incorporar las nuevas tecnologías al Código Penal. Asimismo, el texto de este artículo mereció observaciones respecto de la introducción del verbo típico "obtuviere" por cuanto ello implicaría extender la punición a límites exagerados, ya que en tanto no sea difundido, revelado o cedido el dato o hecho captado, la lesión al bien jurídico protegido es prácticamente insignificante".

El proyecto en su versión de Diputados podría haber impactado en los medios de investigación periodísticos, sobre todo en el periodismo investigativo y en el uso de cámaras ocultas para detener y dar a conocer casos de corrupción. Asimismo habría creado controversias con las actuales medidas de video-vigilancia existentes en el sector público y privado. También podría haber sido usado en casos de agencias de investigación y detectives privados para poner coto a invasiones a la privacidad, aunque a veces estas investigaciones pueden ser legítimas si se realizan dentro del marco legal.

En el derecho comparado las cámaras ocultas han sido controvertidas, habiéndose admitidos en algunas decisiones judiciales su uso por parte de la prensa y considerado ilícitas en otras, sobre todo porque en muchas situaciones significan un avance no consentido sobre la propiedad o la privacidad de terceros35. Pero esto no significa que la solución sea penalizar su uso.

Estafa informática

El proyecto propone como nuevo inciso 16 del artículo 173 del Código Penal, dentro del capítulo sobre las defraudaciones, el siguiente: "El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.".

Pero a diferencia de la redacción de Diputados, el Senado clarifica tanto los medios como el iter criminis. Se explica así la propuesta de cambio "Se conservó la redacción de la sanción de Diputados con dos supresiones: "actuado sin autorización del legítimo usuario", porque se entendió que agrega un elemento al tipo que resulta confuso e innecesario, ya que la autorización no podría excluir la ilicitud de la conducta de defraudar; y "luego de su procesamiento", porque no se encontró el justificativo de fijar el momento técnico de una etapa de la transmisión de datos. Por ello en el (…) presente dictamen no se discriminan esos momentos, dando al juzgador precisión normativa y evitando elementos típicos que lo pudieran hacer incurrir en confusión".

Daño informático

El art. 10 del proyecto incorpora como segundo párrafo del artículo 183 CP, el siguiente: "En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños".

En el contexto informático, destruir o inutilizar quiere decir borrar definitivamente sin posibilidad de recuperación. La respuesta a si esto ocurre o no en un caso concreto dependerá del sistema informático y operativo utilizado. En la mayoría de los sistemas operativos la

acción de borrar no implica que el hecho se produzca indefectiblemente, pues los archivos borrados se almacenan en una carpeta conocida como basurero o trash can. Generalmente para poder concluir la acción de borrado de datos el usuario debe reconfirmar el borrado para eliminar los documentos e incluso en estos casos es posible recuperarlos en algunas situaciones. Por ende la consideración de la destrucción debe ser analizada caso por caso. Existen otras formas de borrado mediante virus informáticos, o programas dañinos que pueden "saltearse" estas seguridades impuestas por los sistemas operativos. También cabría la posibilidad de destruir el hardware (generalmente de menor valor) con la finalidad de destruir los datos o software (de mayor valor).

El hecho que exista un sistema de back up, como sucede en la mayoría de las empresas en modo alguno altera el delito de daño pues la restauración requiere un esfuerzo que ya implica reparar el daño causado.

El delito puede recaer sobre "datos, documentos, programas o sistemas informáticos". Esta es la principal modificación que requería nuestro código penal. La ausencia de tales objetos en la descripción del art. 183 CP llevó en numerosos casos a concluir que su destrucción resultaba atípica.

Además del daño informático tradicional se agrega una nueva modalidad de daño. Se penaliza a quien "vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños". Se entiende que estos programas, como por ejemplo un virus maker o herramientas específicas de destrucción de datos, son potencialmente dañosas. Por ende quien de alguna manera pone en el comercio un programa de tales características, con conocimiento del daño a producir, ayuda de alguna manera a cometer el delito de daño a quien usará la herramienta.

El proyecto, sin embargo, no prohíbe la existencia de estos programas, sino que penaliza a quien los venda, los distribuya o los haga circular o introduzca concretamente en un sistema informático. La redacción da a entender que sería un delito de peligro abstracto, y por ende no requerirá un daño concreto. Entendemos sin embargo que como se sigue exigiendo la presencia de dolo, y en especial del dolo específico de dañar40 (no basta incluso una voluntad genérica: debe tratarse de una intención clara y manifiesta). No quedan aprehendidas por esta figura las conductas donde no hay dolo de dañar.

En cuanto a la posibilidad de incriminar a quienes producen una herramienta que puede eventualmente usarse para crear daños informáticos, el tema se platea con las llamadas tecnologías de doble uso, de las cuales vemos miles de ejemplos en la vida cotidiana: la fotocopiadora, la video casetera, un equipo "doblecasetera", un ipod, un disco rígido, una grabadora de DVD, el software peer to peer, y un largo etcétera de software y hardware que permite copiar obras intelectuales, reproducirlas, difundirlas. Tanto doctrina como jurisprudencia41 coinciden ampliamente en que estas tecnologías no son ilegales ni susceptibles de ser prohibidas si tienen usos sustancialmente legítimos o no infractores, aunque de paso también tengan usos no legítimos42. La solución legal más razonable en estos casos es permitir la existencia de estas herramientas y solamente sancionar su uso en un caso concreto cuando este uso sea ilícito pero permitiendo que coexistan los usos legítimos. Por ende si el programa destinado a causar daños encuentra un uso legítimo, tal uso no será ilegal, en cambio si no es posible encontrarle usos legítimos o que no produzcan daño, no se ve porque no debería prohibirse su distribución.

También esta figura tan amplia de daño informático plantea otros problemas para la protección de la propiedad intelectual cuando se utilizan programas anticopia que dañan, degradan o limitan el funcionamiento del sistema informático. Veamos.

Si un programador inserta un virus en un programa a fin que, en caso de copia, el mismo se active y destruya la información existente en el ordenador es posible considerar la situación como un daño informático además de un abuso de derecho (art. 1071 Código Civil). Si bien el titular de la obra de software está en su derecho de proteger sus intereses como autor o dueño (arts. 1 y 5 ley 11723), dicha facultad no debe extenderse más allá de lo que razonablemente expliciten las leyes, o el contrato que lo relacione con el usuario. Así, cabe plantearse la situación de que el sistema de seguridad anti-copia –conocidos generalmente como dispositivos de "self- help"- sólo se limite a borrar o detener el programa no original (la copia ilícita) dejando intactos los datos del usuario. En tal situación el productor de software no está -a nuestro entender- infringiendo norma de derecho penal alguna para el caso que haya previsto esta facultad en el contrato de licencia, y no haya transferencia de propiedad del software ni de las copias. Si bien en otra ocasión sostuvimos que la vía correcta en ese caso sería demandar judicialmente el secuestro y destrucción de la copia ilegítima, luego de revocar la licencia43, un nuevo examen de la cuestión nos convence de que no resulta necesario recurrir a acción judicial alguno si esto está previsto en el programa adecuadamente.

No creo que este tipo penal pueda aplicarse a los recursos informáticos que inhabilitan o degradan el sistema operativo en caso de copia ilegal de un sistema operativo o programa de ordenador limitando su propia funcionalidad.

Ello es así porque la finalidad de este delito es penalizar al que daña con la intención de alterar datos o sistemas informáticos, por lo que requiere un dolo específico de dañar que no es compatible con la situación comentada, que constituye una legítima defensa de la propiedad intelectual.

La mejor guía para arribar a esta conclusión es interpretar el bien jurídico protegido del delito de daño que es la propiedad. Sabemos que no hay delito si no está afectado el bien jurídico protegido. En estos casos el software pertenece al titular de los derechos de autor que dispone la protección tecnológica determinada, por ende, la propiedad del dueño del ordenador no está afectada ni destruida. No existe el daño sobre bienes propios.

Finalmente, la supuesta víctima no podría alegar que su máquina se encuentra disminuida en su funcionalidad cuando la causa de ello es su propio accionar ilegal que consiste en copiar y usar una obra intelectual -programa de ordenador- sin la autorización de su titular46, lo que genera la falta de funcionamiento pleno del sistema.

Los fabricantes de software suelen recurrir a estos dispositivos de protección como una medida antipiratería. Obviamente, estas medidas disgustan mucho a los usuarios, y hasta hacen incómodo el uso de sistemas informáticos pero son perfectamente legales en la medida en que no se afecte materialmente el hardware o se destruyan datos, programas o contenidos ajenos.

El proyecto de reforma agrega como agravante al Art. 184 CP el siguiente: "Artículo 184.- La pena será de tres meses a cuatro años de prisión, si mediare cualquiera de las circunstancias siguientes: (…) 6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público."

Daño a las comunicaciones

Hemos dado este título a la nueva figura propuesta en el Art. 197 CP porque consideramos que al incluir cualquier clase de comunicación (y no sólo las antiguas telegráficas y telefónicos) la figura no sólo ampara lo público sino cualquier clase de comunicación incluyendo las privadas como el correo electrónico, la voz a través de IP, o los mensajes de chat o de texto a través de celulares (SMS).

Esta reforma es importante porque el tipo anterior, como había dicho la doctrina, estaba teñido de la idea de lo público, ya que lo que se protege es la seguridad pública. Lo que quiso el legislador es ampliar el tipo penal a esos nuevos medios de comunicación con independencia de su naturaleza pública o privada.

El proyecto propone entonces que el nuevo Art. 197 quede redactado así "Será reprimido con prisión de seis meses a dos años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.".

Se trata de una figura dolosa, sobre todo en lo relativo al verbo resistir. No cabe entonces incluir dentro de este tipo de delitos a supuestos de caída de redes o sistemas de comunicaciones por diversos problemas técnicos, ajenos a la intención del operario técnico. Sí en cambio quedarán incluidos los ataques por denegación de servicios

Conclusiones

Esta reforma probablemente requerirá en el futuro de nuevos debates y actualizaciones, pero es muy importante que haya tenido lugar debido a que el Código Penal por su antigüedad no contemplaba ninguna de estos delitos informáticos clásicos.

Clase 12 | Gobierno TI

Herramientas para la implantación del gobierno de las TI

Existen un gran número de herramientas que dan soporte a la administración o gestión de las TI en una organización pero sólo unas pocas tienen por funcionalidad principal el servir de apoyo a la implantación de un sistema de gobierno de las TI integral.

La Tabla 8.1. presenta, a modo de índice, un conjunto de las principales herramientas disponibles.

Resulta interesante la interrelación que existe entre las mismas y cómo algunas proporcionan soporte a otras.

Sin embargo, sólo las herramientas de la primera fila de la Tabla 8.1. son específicas para la implantación de un modelo de gobierno de las TI, el resto de herramientas son útiles en otras áreas (seguridad, gestión de proyectos, gestión de servicios, etc.) que son convenientes abordar como apoyo o soporte de un sistema de gobierno pero son más propias de tareas de gestión de las TI que del propio gobierno de las TI. Aunque, hay que reconocer que el implantar herramientas de gestión de las TI va a generar una cultura organizativa muy propicia para asumir posteriormente un sistema de gobierno de las TI.

Tabla 8.1. Herramientas para la implementación del Gobierno de las TI

Elaboración propia

	ESTÁNDAR INTERNACIONAL	ESTÁNDAR NACIONAL	ESTÁNDAR DE UNA ORGANIZACIÓN
Gobierno de las TI	ISO 38500	AS 8015 COSO	COBIT
Planificación TI		PSI-Metrica 3	
Valor de las TI			Val IT
Gestión Servicios TI	ISO 20000	BS 15000	COBIT ITIL MOF
Gestión de Proyectos		UNE 15781	PMBOK PRINCE2 APMs IPMA
Desarrollo Software	ISO 12207 ISO 15504	Ticket Metrica 3	CMMI Bootstrap
Gestión de Riesgos		AS/NZS 4360 COSO Magerit UNE 71504	
Gestión de Seguridad	ISO 27000 ISO 13335 ISO 13569 ISO 17799 ISO 15408	NIST-800 series BS 7799-2 GAO´s FISCAM German BSI	ASCI-33 COBIT ISF ENV12924 SEI´s OCTAVE SEI´s SW-CMM BPM
Gestión Continuidad	ISO /IEC 25999	PAS-56 AS/NZS 4360 HB 221-2004 BS25999	
Gestión de la Calidad	ISO 9001	EFQM BNQP SixSigma	
Auditoria	ISO 19011		COBIT

ISO/IEC 38500:2008

Esta joven norma está pensada principalmente para el Consejo de Dirección, pretende ayudar a sus miembros a obtener el máximo valor de las TI y de los recursos de información de su organización.

El estándar ofrece un marco de referencia para el gobierno eficiente de las TI, con el objetivo de que los más altos directivos de una organización comprendan y satisfagan sus compromisos legales y obligaciones éticas en relación con el uso de las TI dentro de su organización.

En realidad este estándar es útil para dos colectivos diferentes:

1. Va dirigido a la alta dirección pues les indica la manera en la que deben evaluar, dirigir y monitorizar el uso de las TI en toda la organización.
2. Pero también va dirigido a los gestores de las TI pues les informa y les guía sobre como diseñar e implementar políticas de gestión, procesos y estructuras que den soporte al gobierno de las TI.

El objetivo de este estándar es el de promover el uso eficiente, efectivo y aceptable de las TI en toda la organización:

- Asegurando a los grupos de interés (incluidos inversores, clientes y empleados) que, si se sigue el estándar, se puede confiar en el gobierno corporativo de las TI.
- Informando y guiando a los directivos en el Gobierno de las TI de su organización.
- Proporcionando los fundamentos para una evaluación objetiva del estado del Gobierno de las TI en la organización.

El estándar está compuesto por un conjunto de definiciones estándares, un marco de referencia y unas guías con recomendaciones para el buen gobierno de las TI.

Definiciones estándares

La ISO 38500 incluye un conjunto de definiciones relacionadas con el Gobierno de las TI que sirven como vocabulario común para todos aquellos que conozcan e implementen este estándar. Un ejemplo extraído de dicho vocabulario es el siguiente: "Tecnologías de la Información (TI), recursos necesarios para obtener, procesar, almacenar y distribuir información. Este término también incluye 'Tecnologías de la Comunicación (TC)' y el de 'Tecnologías de la Información y las Comunicaciones (TIC)' ". Este es un buen ejemplo de cómo el vocabulario propuesto por la norma pretende unificar un conjunto de términos utilizados con anterioridad bajo una denominación única y común.

Se recomienda una lectura pausada de este catálogo de definiciones y la asimilación y utilización de los mismos en lo sucesivo como primer paso para cumplir con esta norma.

Marco de referencia

El marco de referencia para el gobierno de las TI incluido en la ISO 38500 se compone, a su vez, de seis principios y un modelo de gobierno.

Principios

Los principios expresan cuales son los comportamientos que deben adoptarse a la hora de la toma de decisiones. Cada principio establece qué es lo que debería ocurrir, pero no indica cómo, dónde o quien debe implantar dichos principios. Estos aspectos dependerán de la naturaleza de la organización. Los directivos deben velar porque se apliquen estos principios.

Los seis principios propuestos, de manera resumida, son:

1. **Responsabilidad**: establecer las responsabilidades de cada individuo o grupo de personas dentro de la organización en relación a las TI.
2. **Estrategia**: hay que tener en cuenta el potencial de las TI a la hora de diseñar la estrategia actual y futura de la organización.
3. **Adquisición**: las adquisiciones de TI deben realizarse después de un adecuado análisis y tomando la decisión en base a criterios claros y transparentes. Debe existir un equilibrio apropiado entre beneficios, oportunidades, coste y riesgos, tanto a corto como a largo plazo.
4. **Desempeño**: las TI deben dar soporte a la organización, ofreciendo servicios con el nivel de calidad requerido por la organización.
5. **Cumplimiento**: las TI deben cumplir con todas las leyes y normativas y las políticas y los procedimientos internos deben estar claramente definidos, implementados y apoyados.
6. **Factor humano**: las políticas y procedimientos establecidos deben incluir el máximo respeto hacia la componente humana, incorporando todas las necesidades propias de las personas que forman parte de los procesos de TI.

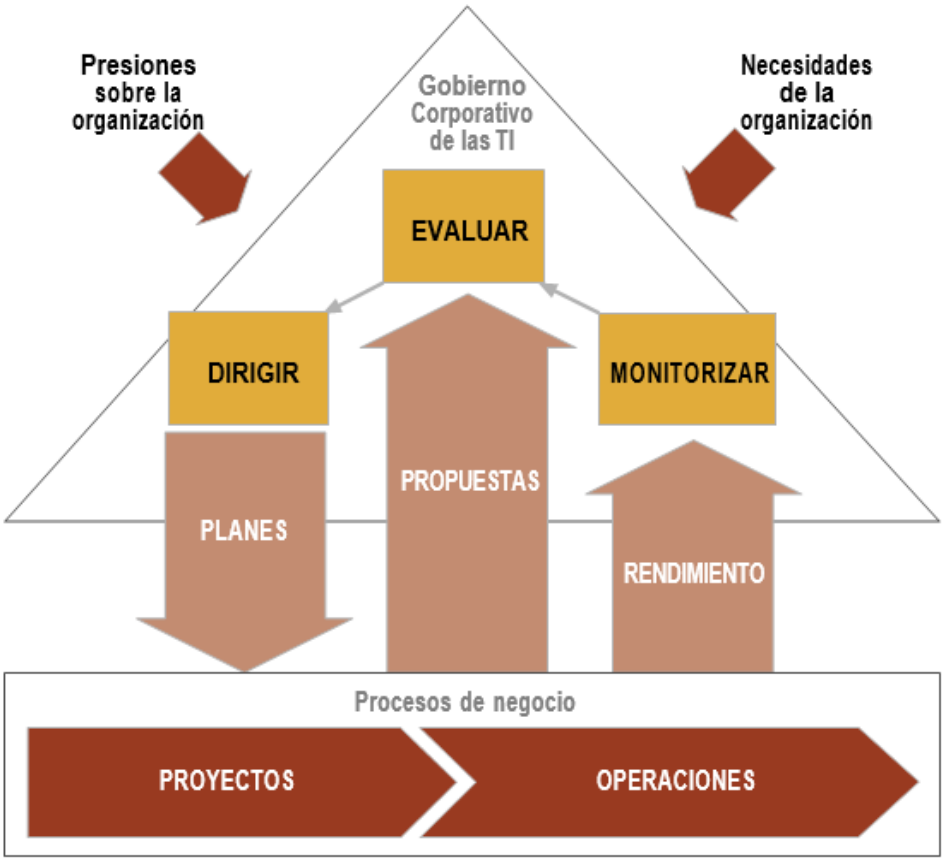
Modelo de gobierno

La norma establece que los directivos deberían gobernar las TI a través de 3 acciones:

- **Evaluar** la utilización actual y futura de las TI.

- **Dirigir** la preparación e implementación de los planes y políticas que aseguren que la utilización de las TI alcanzan los objetivos de negocio.
- **Monitorizar** mediante un adecuado sistema de medida, la adecuación a las políticas, procedimientos y planes establecidos (tanto interna como externamente).

Figura 8.1. Modelo de Gobierno de las TI de la norma ISO 38500
Adaptado de ISO 38500 (2008)



Guía de recomendaciones

El estándar también proporciona un conjunto de recomendaciones para el buen gobierno de las TI y propone una serie de prácticas para implementar los principios descritos anteriormente (tabla 8.3). Las recomendaciones sólo son un punto de partida para los gestores de TI que deben completar estas guías a la hora de implementarlas, identificando cuales son las acciones específicas necesarias para alcanzar los principios.

Te dejo la tabla para que la veas mi rey, pero la va a estudiar dios:

Tabla 8.3. Resumen de las recomendaciones de buen gobierno de las TI de la norma ISO 38500

	EVALUAR	DIRIGIR	MONITORIZAR
RESPOSABILIDAD	- Los modelos y opciones para asignar responsabilidades - Las capacidades de	- Que se lleven a cabo los planes diseñados - Que los directivos	- Ver si están establecidos los mecanismos de Gobierno de las TI

	aquellos que reciben la responsabilidad	reciban la información que necesitan para tomar decisiones	- Comprobar si se comprenden las responsabilidades asignadas - Medir si rinden adecuadamente las responsabilidades asignadas
ESTRATÉGIA	- Los desarrollos de TI para comprobar que darán soporte al negocio en un futuro - Si las actividades de TI están alineadas con los objetivos de negocio - Si se gestionan los riesgos relacionados con el uso de las TI	- Que se diseñen políticas y planes que aprovechen el valor de las TI - Que se innove en TI	- Comprobar si se alcanzan los objetivos en el plazo y con los recursos planificados - Medir los resultados para comprobar que se hayan alcanzado los beneficios esperados
ADQUISICIÓN	- Diferentes opciones con ofertas de TI en relación al coste y al riesgo	- Que el procedimiento de compra sea el adecuado - Que se satisfagan las necesidades de la organización	- Comprobar que las inversiones proporcionan las capacidades esperadas - Ver hasta qué grado se comparte los objetivos de adquisición con el proveedor
DESEMPEÑO	- Las propuestas operativas de los gestores de TI para mantener la capacidad del negocio. - El riesgo de las TI en relación a la continuidad de las operaciones de negocio - El riesgo para la integridad de la información - La eficacia de las decisiones de TI para el negocio - El rendimiento eficiente del sistema de gobierno de las TI	- Que se disponga de suficientes recursos TI - Que se proporcione a la dirección la información correcta y actualizada como soporte de las decisiones	- Ver en qué medidas las TI dan soporte al negocio - Comprobar que la asignación de recursos se prioriza en relación a los objetivos de negocio - Comprobar que se cumplen las políticas y normas establecidas

CUMPLIMIENTO	- En qué medidas se cumple la legislación y las normas internas establecidas - El cumplimiento interno de los procedimientos propios del Gobierno de las TI establecido en la organización	- Que se establezcan mecanismos para comprobar el cumplimiento de leyes, normas y estándares - Que se establezcan políticas que apoyen el uso y la integración de las TI - Que el personal de TI tenga un comportamiento profesional y respete los procedimientos - Que se realice un uso ético de las TI	- Realizar auditorías y redactar informes del rendimiento y cumplimiento - Comprobar que las TI preservan la privacidad y el conocimiento estratégico
COMPONENTE HUMANO	- Que el componente humano está identificado y se tiene en cuenta en todas las actividades TI	- Que las actividades TI sean consistentes con el componente humano - Que sean identificados y reportados por cualquiera los riesgos y oportunidades para que sean estimados por los directivos	- Si se percibe como importante el componente humano - Si se aplican las prácticas adecuadas para hacerlo consistente con el uso de las TI

La ISO 38500 en relación a las universidades

La ISO 38500 tiene un carácter global y es válida para todo tipo de organizaciones, independientemente de su naturaleza, tamaño o situación geográfica, por tanto también es aplicable a las universidades.

Toomey (2009) establece que las organizaciones que deseen implantar la norma ISO 38500 deberían seguir las siguientes recomendaciones, que propongo sean consideradas también por las universidades (rey acá son como 500, así que dejo la última que fue la que resaltaron):

- Reconocer que el pilar fundamental de un sistema de gobierno de las TI son las personas, que tienen necesidades, aspiraciones y un amplio rango de particularidades. Cambiar o implementar un nuevo sistema de gobierno de las TI puede significar que todas las personas de la organización se sitúen en el camino hacia el cambio, que para algunos puede ser un reto demasiado complicado

Esta última tarea es la más complicada y la que puede provocar que falle la implantación del sistema de gobierno de las TI si se confía a las personas inadecuadas.

DOCUMENTO ELECTRONICO Y FIRMA DIGITAL.

A lo largo de la historia de las relaciones humanas nos encontramos con un común denominador cual es la preocupación constante de que las mismas se desenvuelvan en armonía y que los acontecimientos y hechos importantes queden grabados en la memoria colectiva, y además puedan ser probados.

Cuando las relaciones además tienen consecuencias jurídicas, las leyes deben hacerse cargo de la regulación de estas situaciones. Así aparecen normativamente los conceptos de forma y prueba de los actos jurídicos.

FORMA Y PRUEBA

La **Forma** es el elemento esencial del acto jurídico. Es el modo en que el sujeto se relaciona con el objeto. Es la exteriorización de la voluntad, es lo que la hace visible.

En algunos casos, la forma, debe cumplir ciertos recaudos, exigidos por la ley para que el acto tenga validez. Suele llamársela "forma legal". Ej: Transmisión de bienes inmuebles que debe hacerse por escritura pública.

En el Código Civil argentino rige el principio de libertad de formas, pero en realidad, muestra alguna preferencia por la forma escrita.

La **Prueba** es la acreditación de la verdad de un hecho, más precisamente la demostración por alguno de los medios que la ley establece, de la verdad de un hecho del cual depende la existencia del derecho. La prueba de los actos jurídicos es independiente de su existencia.

Medios de prueba.

Los medios de prueba son los elementos que la ley admite con fuerza probatoria, es decir que se pueden usar en juicio para demostrar la autenticidad de un hecho.

Una especie de los medios de prueba lo constituye la llamada "prueba documental", que consiste en acreditar la verdad de un hecho utilizando documentos.

DOCUMENTO

En sentido amplio, documento es toda representación material, verbal o figurativa, destinada e idónea para reproducir una cierta manifestación del pensamiento o representar un hecho, de modo que pueda ser conocido a distancia en el tiempo. A esto habría que agregarle que también ese hecho debe ser apto para producir efectos jurídicos, pues sino, carecería de trascendencia a los fines para lo que es requerido.

Dentro del género documento, encontramos, como especie, a los documentos escritos. A éstos, dentro del Código Civil se los llama instrumentos. A su vez, los instrumentos pueden ser públicos o privados.

La concepción tradicional del documento lo ha asimilado con la escritura, entendiendo por tal, un conjunto de símbolos o caracteres, desarrollados en lenguaje accesible al hombre y aplicado sobre

soporte capaz de receptar una grafía.

Hoy existen otros medios que sin ser escritos documentan hechos y circunstancias probablemente con mayor fidelidad y no son escritos. Ej: fotografías, filmaciones, microfilms, etc.

El **documento** es un **objeto** (cosa), que hace conocer un hecho, que lo **representa**, en contraposición al **testigo**, que lo **narra**.

Soporte

Todo documento requiere un soporte para su representación, es decir un sustrato material sobre el que se asiente la información.

La representación de un hecho, para que tenga valor documental, debe expresarse por un medio permanente, que permita su reproducción, que es la forma de la representación.

El papel, es el más tradicional de los soportes documentales, pero obviamente no puede considerarse el único. A lo largo de la historia los soportes han ido evolucionando desde la piedra hasta los actuales soportes electrónicos.

Esta nueva categoría de soportes ha dado nacimiento a la noción de documento electrónico.

Este puede ser entendido genéricamente como la fijación de información, en un soporte electrónico que permite su recuperación.

En sentido estricto, es el conservado en forma digital, que no puede ser leído por el hombre, sino como consecuencia de un proceso de traducción.

Requisitos de los documentos escritos.

Todo documento, para tener plena eficacia jurídica, debe tener requisitos de autoría, autenticidad, integridad y permanencia.

Autoría significa que ese documento le puede ser imputado a un autor determinado.

Autenticidad: implica que el documento no ha sido falsificado ni adulterado.

Integridad: quiere decir que el documento debe estar completo.

Permanencia: está referido a la perdurabilidad del soporte.

El papel ha sido un razonable soporte físico hasta ahora. Una de las críticas más importante al documento electrónico, es la duda sobre el carácter de permanente por la posibilidad de reinscripción que presenta.

La discusión más fuerte que se planteó acerca del documento electrónico fue las de si se lo podía considerar documento escrito.

Del concepto tradicional de documento escrito se desprende que éste tiene soporte, grafía y contenido.

- **Soporte** (papel)
- **Grafía** (lenguaje)
- **Contenido** (información que representa).

El documento electrónico también tiene

- **Soporte** (cintas, discos)
- **Grafía**: (Formato o código en que se registra la información sobre el soporte)
- **Contenido** (información que representa)

La discusión doctrinaria sobre si debe considerárselo documento escrito ha quedado zanjada después de la sanción de **la ley de firma digital** que en su **Art. 6** define al documento digital y aclara que "***un documento digital también satisface el requerimiento de escritura***".

Esto quiere decir que cuando las leyes hablan de documento escrito, el concepto debe ampliarse para incluir al documento digital.

LA FIRMA COMO ELEMENTO DE SEGURIDAD DOCUMENTAL.

La **firma** es una **forma de exteriorización** de la **voluntad** humana. Es un **signo personal autógrafo**, trazado por la mano del autor, que sirve para **informar** sobre la **identidad** del autor de la declaración de voluntad, así como del **acuerdo** de éste con el **contenido** del acto y que luego sirve para **probar** la autoría.

La firma manuscrita tiene validez jurídica en nuestra sociedad y cultura pues en la tradición de su uso se la considera aceptable para identificar al autor de un documento y simultáneamente asegurar la integridad del contenido de ese documento, cuando se cumplen las siguientes condiciones:

- Que esté escrito con tinta indeleble y en soporte papel, tal que una enmienda o raspadura que altere la información escrita sea visible y evidente.
- Que posea márgenes razonables que contengan los renglones escritos, tal que cualquier escritura adicional sea visible y evidente.
- Que la firma manuscrita esté colocada delimitando la información escrita, tal que no sea posible agregar texto escrito excepto a continuación de la firma manuscrita.
- Que el firmante utilice siempre la misma o similar firma manuscrita para firmar los documentos de su autoría.
- Que la firma manuscrita sea suficientemente compleja tal que su falsificación devenga no trivial.
- Que existan peritos caligráficos que puedan detectar las falsificaciones con un razonable grado de certeza.

La falla de cualquiera de esto puntos torna inseguro al mecanismo de firma manuscrita para documentos en soporte papel permitiendo así a su autor (por ejemplo) repudiar la autoría de los documentos que le son atribuidos.

Teniendo en cuenta la importancia que tienen la firma para la eficacia de la prueba documental y atento a la existencia del documento digital en la vida negocial, se hizo necesaria la sanción de una ley que reglamentara y diera validez al mecanismo que sirve para firmar documentos digitales.

Así, en diciembre de 2001 se sancionó la ley 25.506 de firma digital.

LEY DE FIRMA DIGITAL 25.506

Le ley reconoce el empleo de la firma electrónica y la firma digital y les otorga eficacia jurídica.

Establece como principio que cuando una ley requiera una firma manuscrita, esa exigencia puede ser cumplida igualmente por una firma electrónica o digital pero fija restricciones para algunos actos jurídicos que quedan excluidos de la posibilidad de usar firma digital.

Estos actos son:

- Disposiciones por causa de muerte. Ej. Testamentos.
- Actos jurídicos del derecho de familia. Ej. Reconocimiento de paternidad.
- Actos personalísimos en general. Ej. Disposiciones sobre el propio cuerpo.
- 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.

Definición

La ley distingue entre firma electrónica y firma digital:

- **Digital**: Art. 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".*
- **Electrónica**: Art. 5: *"Conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez."*

La **diferencia** se traduce en **distintos efectos jurídicos** de uno y otro tipo de firma ya que de acuerdo a los arts. 7 y 8 **la digital goza de presunción de autoría e integridad**, es decir la carga de la prueba recaerá sobre la persona que alega la falsedad de un documento firmado digitalmente o que el mismo ha sido firmado por interpósita persona.

Podemos decir entonces que:

a.- La **firma** es la **prueba de la manifestación de la voluntad que permite imputar la autoría e identificar al firmante de un instrumento**.

b.- Firma electrónica: es un **método** o símbolo **basado en medios electrónicos utilizado o adoptado por una persona con la intención de vincularse o autenticar un documento**. Es una forma de manifestar la voluntad mediante medios electrónicos que d**ebe ser probada por quien invoca** su validez.

c.- **Firma digital**: es la **firma electrónica** que **utiliza una técnica segura** que permite **vincular e identificar** fehacientemente al **firmante** del documento digital garantizando la **autenticación**, **integridad** y **no repudio** del documento firmado. Es una forma segura y verificable de manifestar la voluntad mediante medios electrónicos.

Validez.

Una firma digital es válida si cumple con los siguientes requisitos:

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

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

c) Que dicho certificado haya sido emitido o reconocido, por un certificador licenciado.

Certificados.

Un documento digital firmado digitalmente no sólo necesita ser verificado en cuanto a su integridad, sino también en cuanto a la identidad del firmante. Esta identificación se produce a través de los certificados digitales.

Un certificado digital es un documento digital firmado digitalmente por un tercero (Certificador) que vincula los datos de verificación de firma a su titular.

Para que produzcan los efectos jurídicos de la firma digital deberán provenir de un Certificador Licenciado. Si emanaren de certificadores no licenciados, tendrán los efectos jurídicos de la firma electrónica.

Certificadores licenciados.

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.

Para ello debe contar con una licencia otorgada por el ente licenciante (Ente Administrador de Firma digital).

Sus funciones son:

- Emitir certificados digitales de acuerdo a lo establecido en sus políticas de certificación, y a las condiciones que indique la ley.
- Identificar inequívocamente los certificados digitales emitidos.
- 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.
- Revocar los certificados digitales por él emitidos en los casos que determinen la ley.
- 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.

Autoridades de registro.

Los Certificadores Licenciados podrán delegar en Autoridades de Registro las funciones de validación de identidad y otros datos de los suscriptores de certificados y de registro de las presentaciones y trámites que les sean formuladas, bajo la responsabilidad del Certificador Licenciado y cumpliendo las normas y procedimientos establecidos por la reglamentación.

ORGANIZACION INSTITUCIONAL

Autoridad de Aplicación.

La Autoridad de Aplicación, es decir, a cargo de quién están todas las cuestiones relacionadas con la implementación de la firma digital, es la Jefatura de Gabinete de Ministros.

Su función es determinar las normas y los procedimientos técnicos para la generación, comunicación, archivo y conservación del documento digital o electrónico.

Entre otros deberá establecer:

- Los estándares tecnológicos y de seguridad aplicables en consonancia con estándares internacionales.
- Los procedimientos de firma y verificación en consonancia con los estándares tecnológicos definidos conforme el inciso precedente.
- Las condiciones mínimas de emisión de certificados digitales.
- Los procedimientos mínimos de revocación de certificados digitales cualquiera que sea la fuente de emisión, y los procedimientos mínimos de conservación de la documentación de respaldo de la operatoria de los certificadores licenciados, en el caso que éstos cesen su actividad.
- El sistema de auditoría, incluyendo las modalidades de difusión de los informes de auditoría y los requisitos de habilitación para efectuar auditorías.
- Las condiciones y procedimientos para el otorgamiento y revocación de las licencias.
- Exigir las garantías y seguros necesarios para prestar el servicio previsto.

UNIDAD VII

RÉGIMEN LEGAL DE LAS BASES DE DATOS.

700. INTRODUCCION.

Siempre ha existido en la sociedad acumulación de información, siempre han existido ficheros de distintos tipos y de distintas características; lo que la informática evidentemente ha aportado son elementos específicamente diferenciales que hacen a la estructuración y al manejo de la información.

Este aporte se plasma en tres grandes ámbitos:

1. **Concentración de la información**: lo nuevo que aporta el instrumental informático al manejo de la información es la posibilidad de concentrar en grandes bancos de datos enormes volúmenes de información de distinto tipo.
2. **Recuperación de la información**: la posibilidad de recuperar rápida y eficientemente la información es el segundo aporte esencial de la informática los bancos de datos.
3. **Transferencia y entrecruzamiento de la información**: este aspecto implica la posibilidad del envío, transferencia o transporte de la información, entrecruzamiento de la información contenida en un banco de datos, entre bancos de datos o entre sistemas ubicados inclusive en jurisdicciones nacionales diferentes.

Este impacto de la informática sobre las bases de datos, importa la aparición de nuevos problemas con consecuencias jurídicas a los que el derecho debe dar respuestas. La determinación del régimen jurídico de las bases de datos está íntimamente ligada a la compresión de dichos problemas que requieren y deben tener soluciones específicas desde el ámbito jurídico.

701. CLASIFICACIÓN

Existen varios criterios para clasificar a las bases de datos. Entre los más comunes se pueden mencionar los siguientes tipos:

Públicos o privados: La característica distintiva es la determinación de de quién depende la gestión de un banco de datos específico. Los bancos de datos públicos, son aquéllos dependen de algún organismo de la administración pública de los estados (nacionales, provinciales o municipales). El resto son privados.

Textuales o referenciales: Esta clasificación de los bancos de datos es en función de las características esenciales de diseño, de estructuración. Está relacionada con la forma en que la información contenida en un banco de datos determinado esté cargada, que puede ser en texto completo, o en forma referencial, es decir, que esté incluida una referencia al contenido esencial del documento o de la información.

Locales o generales: Las bases de datos pueden ser de carácter local, orientadas con información que responda al interés específico de un ámbito geográfico determinado o de carácter general.

702. PRIVACIDAD. HÁBEAS DATA.

El tema de la privacidad relacionada a las bases de datos ha preocupado a los hombres desde hace bastante tiempo, más allá que la primera referencia jurídica dista a fines del siglo XIX, que han tratado de encontrar una adecuada protección a su vida privada y a ciertos aspectos que no solo tienen que ver con el individuo sino también con su entorno familiar, frente a la intromisión arbitraria de otras personas.

El derecho a la Privacidad, es el derecho que tiene toda persona a que se la deje sola, se la deje alejarse en aquellos aspectos de su vida en la que considera sólo reservados a su conocimiento. Pero la irrupción de las tecnologías y las comunicaciones alteraron profundamente el sentido y la orientación de la protección vida que poco a poco el Derecho Positivo había ido estructurando en relación a la privada

Desde el punto de vista normativo, este derecho empezó a ser regulado desde la década del '70. Suecia, Francia, Alemania fueron algunos de los países pioneros en estos temas.

El impacto de las modernas tecnologías no solo se ha producido sobre el clásico derecho a la intimidad, el derecho a la privacidad, sino también sobre otros derechos personalísimos como son el derecho al honor, el derecho a la imagen, el derecho a la identidad dinámica y además, tiene potencialidad de afectar también los derechos de determinados sujetos colectivos como pueden ser la colectividad, una nacionalidad de determinado género o los afectados por algún tipo de enfermedad.

Esto se relaciona directamente con lo que se entiende por datos de carácter personal.

Son todas aquellas informaciones susceptibles de ser atribuidas a una persona y que tienen aptitud para identificar a esa persona. En tal sentido podemos distinguir aquellos datos referidos a personas pero que han sido sometidos a un proceso de disociación, es decir que se les han extraído, eliminado o bloqueado aquellos aspectos de la información que permitirían identificar a uno o más sujetos.

Cuando se habla de datos de carácter personal se está refiriendo a un conjunto de informaciones acerca de una realidad específica, que es en principio un ser humano, pero que en lo que respecta a la protección de la ley se ha extendido incluso a personas de existencia ideal y que permite identificarlo a partir precisamente de la información y los datos

que están allí contenidos.

Sobre el tratamiento que este tipo de información puede tener es que se ha tratado de establecer principios reguladores, principios que ponen límites y establecen pautas sobre cómo debe ser el tratamiento de este tipo particular de información, que a partir de la aplicación de las tecnologías informáticas y las telecomunicaciones, adquieren una dimensión y una potencialidad riesgosa que era desconocida anteriormente.

703. PRINCIPIOS REGULADORES DEL TRATAMIENTO DE DATOS PERSONALES

703.a. LICITUD

Nadie puede, en principio, recolectar datos, acopiar información, que no tenga un propósito socialmente válido. Este principio apunta a que nadie pueda tener datos de un sujeto si no es para aplicarlos a un fin socialmente válido y lícito es decir, permitido por el ordenamiento jurídico. Este primer principio es el que invalida nulifica, excluye del ordenamiento jurídico a cualquier base de datos que no responda a estos criterios y a estos parámetros.

Para tener en claro este principio se deben precisar cuáles son los aspectos de la vida de una persona que deben ser preservados de manera tal que, quien violente esta reserva o esta valla, esté incurriendo en una actitud ilícita o esté efectuando una recolección de datos con un fin socialmente inválido.

Un aspecto fundamental está en el Art. 18 de la Constitución Nacional que protege los papeles y la correspondencia privada, para tener una idea de cómo desde antaño se ha entendido que existe una zona de reserva, un aspecto de la personalidad que toda persona tiene derecho a excluir a los demás de su conocimiento. Sin ninguna duda las modernas tecnologías y en particular por ejemplo el correo electrónico o la navegación a través de Internet han complicado este panorama. También se encuentra un ejemplo en la Ley de Derechos de Autor o de Propiedad Intelectual, la Ley 11.723 (tengamos en cuenta que es del año 1933) que veda aún hoy el uso de la fotografía de una persona sin su autorización, salvo cuando es para fines de divulgación científica o educativa y esto por supuesto respetando determinados contextos.

Cuando hablamos de datos no nos estamos limitando sólo a la información contenida en un formato texto, sino que también estamos incluyendo las imágenes, a la voz y a otras capturas de este comportamiento declaraciones de voluntad en cualquier lenguaje que sea reproducible frente a terceros.

703.b. FINALIDAD

Este principio implica que los datos deben ser recogidos con una finalidad explícita y no ser tratados posteriormente con una finalidad distinta o de una manera incompatible con el propósito con el que fueron requeridos originariamente, salvo cuando se trata de darle a esos datos un tratamiento histórico, estadístico o científico y siempre y cuando los Estados ofrezcan las garantías oportunas para ello.

703.c. PERTINENCIA

Nadie tiene derecho a requerir información que no sea pertinente, es decir, que no vaya a cumplir alguna finalidad directamente vinculada al propósito que se ha declarado al requerir esta información.

703.d. Exactitud

El dato que no debe ser ni equívoco ni ambiguo. Es decir, en el dato personal el rigor en su selección, en su tratamiento y en su difusión es mucho mayor que cuando uno puede manejar algún otro tipo de información. Un dato inexacto, por desactualizado o por incompleto, puede convertirse en un dato tremendamente perjudicial, aún cuando en la parcialidad que exprese el dato sea cierto, sea verídico

703.e. Datos no excesivos

Los datos, por otro lado, deben ser conservados en forma identificable sólo durante el período que sea indispensable para que pueda identificarse el sujeto.

703.f. Confidencialidad

La regla en materia de datos de carácter personal debiera ser la confidencialidad, no la publicidad. Esto no porque no sea posible que determinados datos de carácter personal tengan carácter público. De hecho un conjunto de circunstancias que rodean a las personas, -nombre, profesión, en algunos casos domicilio o teléfono o eventualmente la dirección de correo electrónico- en muchos casos se desprende de la manera en que han sido proporcionados, que no hay una pretensión de que sean reservados, todo lo contrario, están expuestos a propósito para que sean conocidos, para permitir la comunicación con los titulares de esos datos, su ubicación, su hallazgo, etc. Pero esto debiera ser siempre el resultado de una operación previa voluntaria.

Por su parte el responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada la relación con el titular del archivo de datos.

Según la ley cualquier obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

Este principio lleva a otro de los principios fundamentales en esta materia que es el del consentimiento.

704. PRINCIPIO DEL CONSENTIMIENTO.

Los datos de carácter personal sólo pueden ser almacenados y difundidos por terceros cuando ha mediado un consentimiento, que en algunos casos deberá ser expreso, libre e informado tal como señalan la mayoría de las legislaciones.

La ley 25.306 que es la que regula la protección de los datos personales, establece que no es necesario el consentimiento cuando: a) Los datos se obtengan de fuentes de acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes.

En todos los demás casos el titular debe prestar su consentimiento libre, expreso e informado, que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo con las circunstancias. Si esta condición no se cumple el tratamiento de esos datos

será ilícito.

El consentimiento sólo es válido cuando se le ha notificado previamente a la persona cuál es la finalidad de esa recolección, de esa operación de juntar información sobre esa persona y además se le ha advertido para qué se va aplicar, para qué se va a utilizar esa información y cuáles son las consecuencias de negarse a brindar esta información y además deben señalar cuáles son los posibles receptores de esa información.

El consentimiento puede considerarse implícito (o no ser necesario como dice la ley) cuando la información resulta necesaria para la ejecución de un contrato en el cual el interesado es parte, o para la aplicación de alguna medida precontractual adoptada precisamente a petición del interesado, o cuando se trata del cumplimiento de una obligación a la que esté sujeta el responsable de los datos, o en una expresión que la ley argentina ha recogido un poco ambiguamente, cuando sea necesario para proteger el interés vital del interesado.

Se excluye esa obligación del consentimiento de interesados cuando los datos se obtengan de fuentes de acceso público irrestricto.

Otra de las excepciones es que se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.

Tampoco es necesario el consentimiento cuando se trate de listados cuyos datos se limiten a nombre, documento de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio

Existe una categoría de datos que requieren un tratamiento especial y que se ha identificado en el mundo entero como *datos sensibles*.

705. DATOS SENSIBLES

En general se entienden incluidos en esta categoría de datos sensibles, a los datos referidos a condiciones políticas, ideológicas, religiosas, cuestiones raciales y algunos aspectos vinculados con la salud o con la conducta sexual. Esta enumeración ha sido reproducida en nuestra ley.

Pareciera que no todos estos datos tienen la misma importancia como datos sensibles. Tienen quizás una connotación y un riesgo mucho mayor los datos referidos a la salud. En esta materia la horizontalización de los negocios y las actividades lucrativas vinculadas a la salud, que no sólo están concentradas en las empresas prestadoras de servicios de salud o de medicina prepaga o de seguros de salud, sino que tienen impacto en la mayoría de la actividad aseguradora, no sólo de los seguros de riesgos de trabajo, las administradoras de fondos de jubilaciones y pensiones, los seguros de vida, los seguros de retiro, sino también las políticas de empleo en el acceso al empleo, es donde más hay que trabajar y precisar los conceptos.

Para tener una idea por ejemplo nuestro país tiene una ley, la Ley N° 23.798 de lucha contra el SIDA que establece criterios muy rigurosos y precisos de confidencialidad en el tratamiento de los resultados y de la detección de una persona que conviva con HIV o que esté enferma de SIDA, e incluso además de establecerlo la ley, el decreto reglamentario que rige en la Argentina es muy preciso sobre cómo deben conservarse los datos y a quienes son los únicos sujetos que se está autorizado a transmitirle esta información que debe ser en un contexto de información adecuada a nivel cultural del receptor, que apunten fundamentalmente a su tranquilidad y a su contención psicológica y a formar parte de su tratamiento y en modo alguno pueden convertirse por impericia o incluso por dolo en un elemento de marginación o discriminación.

706. DERECHOS RELACIONADOS A LOS DATOS CONTENIDOS EN BASES DE DATOS

La ley establece una serie de derechos que tienen los titulares de los datos respecto de esos datos obrantes en bases de datos

707. DERECHO DE ACCESO

Implica el conocimiento cierto de los datos personales que sobre uno tengan terceros. De este se desprenden los derechos de rectificación, actualización, supresión o confidencialidad.

Este derecho puede instrumentarse por vías administrativas o mediante una acción judicial.

El art. 14 de la ley argentina específicamente plantea que el titular de los datos, previa acreditación de su identidad, tiene derecho de solicitar y obtener información de los datos personales incluidos en los bancos de datos públicos o privados destinados a proveer informes.

Por titular de los datos se entiende, en los términos de la ley, que es *toda persona física – en el caso de la ley argentina agrega o de existencia ideal – con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley*.

El responsable, es quien administra, quien es titular de un banco de datos, de una base de datos y el usuario (que puede ser quien ha recibido esta información y la está utilizando, por ejemplo, para decidir si una persona es apta o no para un empleo o para un cargo docente, para un cargo público o para otorgarle un crédito), deben proporcionar la información solicitada dentro de los 10 días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido o se haya evacuado la información o esta se estimara insuficiente, se puede iniciar la acción judicial (acción de hábeas data).

El otro requisito que pone este art. 14 es que el derecho de acceso al que se refiere este artículo solo puede ser ejercido en forma gratuita a intervalos no inferiores a 6 meses, salvo que se acredite un interés legítimo al efecto.

La información debe ser suministrada en forma clara, sin códigos, sin encriptamientos, sin ocultamientos, sin determinadas palabras que uno deba tener que interpretar y en su caso acompañada de una explicación, en leguaje accesible al conocimiento medio de la población de los términos que se utilicen. La información no basta transmitirla tal como está registrada en el banco de datos, sino que debe ser adaptada a un lenguaje claro, comprensivo que no genere dificultades para un estándar medio cultural.

Finalmente el método empleado para suministrar la información la ley lo establece en forma muy amplia, puede ser suministrado por escrito, telefónicamente, por medios electrónicos u otros medio idóneo a tal fin.

708. DERECHOS DE RECTIFICACION, ACTUALIZACION O SUPRESIÓN.

En este sentido la primera referencia debe ser a la Constitución al Art. 43, párrafo 3º que establece que además de este derecho de acceso al que nos hemos referido previamente, toda persona tiene derecho a la rectificación, actualización o supresión de los datos que sean inexactos o falsos o que sean discriminatorios.

El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o

actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo que fija la ley.

709. DERECHO A LA SEGURIDAD EN LA CONSERVACION

Es el derecho a que los datos no sólo no sean conocidos o no tengan acceso a ellos quienes no están autorizados o quienes por la naturaleza de los datos no debieran tener acceso a ellos, sino que además los datos sean conservados adecuadamente.

Esto introduce un conjunto de requisitos de naturaleza técnica, que prácticamente todas las legislaciones imponen, y que también lo establece nuestra norma nacional la 25.326 y que serán motivo seguramente de la reglamentación cuáles son las pautas que deberán observar los responsables de ficheros y de bancos de datos para garantizar la seguridad de los datos de carácter personal que acumulen y procesen.

710. CESION DE DATOS O TRANSFERENCIA DE DATOS.

Los datos personales objeto de tratamiento como regla general no pueden ser cedidos.

Si lo fueren, tiene que serlo para el cumplimiento de los fines directamente relacionados con el interés legítimo del que cede y del que los recibe.

Cualquier cesión debe contar con el con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión y sobre la identidad de a quién le son cedidos los datos.

El consentimiento del titular para la cesión es revocable en cualquier momento.

Según la ley el consentimiento no es exigido cuando:

a) Así lo disponga una ley;

b) En los mismos supuestos en que no es necesario para la recolección.

c) Se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias;

d) Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados;

e) Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables.

En cuanto a la transferencia internacional de los datos, en principio sólo puede hacerse cuando los países u organismos internacionales o supranacionales, proporcionen niveles de protección adecuados.

También puede hacerse en los siguientes supuestos:

a) Colaboración judicial internacional;

b) Intercambio de datos de carácter médico.

c) Transferencias bancarias o bursátiles.

d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte;

e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

711. RESPONSABILIDAD DE LOS OPERADORES DE BASES DE DATOS

En primer lugar, la ley establece una obligación clara para todo aquel que manipule una base de datos de carácter personal, de adecuar su operatoria a la normativa y por otro lado la ley establece tres niveles diferenciales de responsabilidad.

1. En primer lugar la responsabilidad patrimonial, enormes multas administrativas y por otro lado la responsabilidad por eventuales daños y perjuicios causados a terceros.

2. El segundo nivel de responsabilidad es el que se denomina responsabilidad en cascada, es decir la organización que manipule datos de carácter personal no es responsable sólo por lo que hace con esos datos, sino que también es responsable por la acción del tercero cesionario de esos datos que viole también los principios establecidos en la norma

3. El tercer nivel de responsabilidad es la responsabilidad penal. La ley incluye tres nuevos tipos penales que incriminan a aquel gestor de un banco de datos personal que viole los principios establecidos en la norma.