DERECHO DE LAS NUEVAS TECNOLOGÍAS

Informática, es un conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información con miras a una adecuada toma de decisiones.

Informática jurídica, es la técnica interdisciplinaria que tiene por objeto el estudio e investigación de información jurídica, así como a la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación.

Clasificación de la informática jurídica

• Informática Jurídica Documentaria (Almacenamiento y recuperación de textos jurídicos)

• Informática Jurídica de Control y Gestión (Desarrollo de actividades jurídico-adjetivas)

• Sistemas Expertos Legales o Informática Jurídica Metadocumentaria (Apoyo en la decisión, educación, investigación, redacción y previsión del derecho)

Informática Jurídica Documentaria: Se trata de crear un banco de datos jurídicos relativo a cualquiera de las fuentes del derecho (menos la costumbre) a efecto de interrogarlo con base en criterios propios acordes con esa información y su relevancia jurídica.

La finalidad de la Informática en un sistema documentario: Consiste en encontrar lo más rápida y pertinentemente posible la información que ha sido almacenada. El conjunto de esas informaciones constituye el banco de datos.

Informática Jurídica de Control y Gestión: Abarca los ámbitos jurídico-administrativo, judicial, registra y despachos de abogados. Tiene como antecedentes el tratamiento de textos jurídicos mediante el uso de procesadores de palabra y, por otra parte, las experiencias obtenidas en materia de automatización de registros públicos.

- Su uso en la administración publica
- Su uso en los órganos jurisdiccionales
- Su uso en despachos y notarias

INFORMATICA JURIDICA METADOCUMENTARIA: Llamada así porque trasciende más allá de la esencia de los fines documentarios propiamente dichos.
Sus ámbitos principales de injerencia son cinco:

1. Ayuda a la decisión
2. Ayuda a la educación
3. Ayuda a la investigación
4. Ayuda a la previsión
5. Ayuda a la redacción

Derecho informático, es una rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática). Es notorio que la clasificación del derecho informático obedece a dos vertientes fundamentales: la informática jurídica y el derecho de la informática.

Derecho de la Informática, es el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática.
Resulta válido decir que es un conjunto de leyes en cuanto que, si bien escasos, existen varios ordenamientos jurídicos nacionales e internacionales con alusión específica al fenómeno informático. Normas en virtud de aquellas que integran la llamada política informática, la cual, presenta diferencias respecto a la legislación informática. Principios en función de aquellos postulados emitidos por jueces, magistrados, tratadistas y estudiosos respecto del tema. Por otra parte, se refiere a hechos como resultado de un fenómeno aparejado a la informática inimputable al hombre. Por último, se alude a actos como resultado de un fenómeno directamente vinculado con la informática y provocado por el hombre.

Política Informática, para un desarrollo informático adecuado es necesario planificar por medio de normas que a su vez conforman una política diferente de una legislación en cuanto a que esta última se refiere a aspectos más específicos.
Así entre esta política informática algunos de los principales puntos contemplados son el adecuado desarrollo de la industria de construcción de equipos de cómputo y de programación; por otra parte, la planeación, difusión y aplicación del fenómeno informático, la contratación gubernamental de bienes y servicios informáticos, la formulación de normas y estándares en materia informática, y el control de importaciones y exportaciones sobre equipos, accesorios y programas de computadoras, etc.; esto no es suficiente para mantener a la informática en los términos idóneos de crecimiento. En México se tiene el Plan Nacional de Desarrollo y los programas sectoriales correspondientes como muestras más evocadoras en donde se sustenta la política informática.

Legislación Informática, es un conjunto de reglas jurídicas de carácter preventivo y correctivo derivadas del uso (fundamentalmente inadecuado) de la informática, es decir, aquí se trata de una reglamentación de puntos específicos, pero esta circunstancia implica las siguientes consideraciones:
• Si se recurriría a un cuestionamiento de las reglas existentes para determinar si es posible su aplicación análoga frente al problema o si sería necesaria una ampliación en cuanto a su ámbito de cobertura.
• Esperar la evolución de la jurisprudencia dada la creciente presentación de casos ante los órganos jurisdiccionales en lo que se fijen pautas resolutorias o al menos conciliatorias.
• Crear un cuerpo de nuevas reglas integrándolas a ordenamientos ya existentes, o que den lugar a una nueva ley de carácter específico.

Dicha reglamentación deberá contemplar las siguientes problemáticas:

1. Regulación de la información: ya que la información como un bien requiere un tratamiento jurídico en función de su innegable carácter económico.
2. Protección de datos personales: es decir, el atentado a los derechos fundamentales de las personas provocado por el manejo inapropiado de informaciones nominativas.
3. Regulación jurídica de internet: con el favorecimiento o restricción de los portales en internet.
4. Propiedad intelectual e informática, con los temas referentes a protección de los programas de cómputo y regulación de nombres de dominio, ambos derivados de las acciones de “piratería” o “ciberocupación”.
5. Delitos informáticos: la comisión de actos ilícitos en los que se tengan a las computadoras como instrumentos o fin.
6. Contratos informáticos: en función de esta categoría contractual particular con evidentes repercusiones fundamentalmente económicas.
7. Comercio electrónico, nueva forma de comercialización automatizada de bienes y servicios de todo tipo a través de internet. Se incluye el subtema de firma electrónica.
8. Aspectos laborales de la informática, como aquellos problemas laborales suscitados por la informatización de actividades. Ergonomía y teletrabajo.
9. Valor probatorio de los documentos electrónicos: referido a la aceptación y valoración de estos documentos como medio de prueba.

Gobierno Electrónico, es un concepto de gestión que fusiona el empleo adecuado y acentuado de las tecnologías de la información y comunicación, con modalidades de gestión y administración, como una nueva forma de gobierno.

Programa de Gobierno Electrónico, es ante todo un proyecto de políticas públicas en el cual se imaginan escenarios, se programan acciones y se actúan relaciones eficientes dentro de la administración y en referencia a los ciudadanos y las empresas.

El Gobierno Electrónico se desdobla en los siguientes rubros:

- E-administración (administración electrónica). Este término hace referencia a aquellos mecanismos electrónicos que permiten la prestación de servicios públicos de la administración, tanto a los ciudadanos como a las empresas.

- E-democracia (democracia electrónica). Son procesos electrónicos o informáticos que permiten la participación ciudadana en la vida política mediante el uso de las TIC, ya sea en forma directa en la toma de decisiones políticas o por medio de sus representantes.

- E-gobierno (gobierno electrónico en sentido estricto). Abarca desde la simple puesta de documentos en la red hasta una integración completa entre ciudadanos y distintos organismos de la administración, así como la

participación de aquéllos en la toma de decisiones políticas y, por tanto, engloba los conceptos de e-democracia y e-administración

Cibertribunales, tienen como propósito servir de mediadores en los litigios derivados del uso de internet (comercio electrónico, propiedad intelectual, protección de la vida privada, etc.). estos tribunales permiten a las partes interesadas elegir de entre una cantidad de expertos (en ocasiones académicos) aquellos que propondrán soluciones a los conflictos, sustentados en los textos internacionales más avanzados en la materia.

Los sistemas alternativos de solución de disputas (ADR, POR SUS SIGLAS EN INGLES), como el arbitraje, la mediación y la conciliación, presentan claros beneficios y ventajas prácticas en relación con los procesos estatales, en particular para la solución de conflictos dentro de estructuras digitales.

Algunos de sus principales beneficios son:

- Autonomía e la voluntad de las partes.
- Posibilidad de elegir un conciliador o árbitro neutral en otros países
- Posibilidad de utilizar tecnologías e infraestructuras tecnológicas muy avanzadas
- Procesos extrajudiciales muy cortos, simples y flexibles (manteniendo todos los derechos de las partes)
- Trabajo y discusión en tiempo real al tratarse de solución on line de conflictos.
- No hay posibilidad de prolongar los procesos mediante apelación.
- Costos mucho más bajos
- Privacidad y confidencialidad durante el proceso y después de él
- Posibilidad de que expertos evalúen el caso y dicten el laudo (esto es particularmente importante en casos de comercio electrónico y nuevas tecnologías)
- Posibilidad de que un laudo dictado en un país sea válido en cualquier otro país (tratados internacionales)

Arbitraje, es la única solución viable para la solución de los litigios plantados por un comercio electrónico forzosamente internacional, y el arbitraje en línea es el único mecanismo que puede garantizar una adecuación entre los costos de la justicia y lo

que está en juego en los contratos internacionales que ya no son privativos de los grandes grupos. Como sucede con las normas materiales aplicables a los contratos, las normas consensuales que facilitan la solución de litigios se alejan con rapidez de cualquier tipo de recurso a las normas de procedimiento de un sistema jurídico particular. En menor medida, esas disposiciones para la solución de litigios también tienden a estar determinadas por los usos de la industria en cuestión. Si en un futuro el papel de las asociaciones de comerciantes se combina con el de las grandes plazas de mercado electrónicas, cabe pensar que el arbitraje se transformara en jurisdicción de derecho común.

Información: Elemento susceptible de ser transmitido por un signo o combinación de signos; para los efectos informáticos que nos ocupa, lo entenderemos como un proceso físico-mecánico de transmisión de datos, cuyo dato es el elemento referencial acerca de un hecho. En sentido general, un conjunto de datos constituye una información.

- Cualitativamente: Se ha concebido a la información como el contenido de lo que es objeto de intercambio entre el sujeto y el mundo externo, de tal nodo que se presenta un conjunto de datos como elemento de las relaciones del hombre y tendiente a una ordenación, es decir desde este punto de vista la información constituye un factor de organización.
- Cuantitativamente: La información es la medida de disminución de incertidumbre del sujeto respecto a los objetos, de aquí que se hable de una entropía en cuanto al nivel de desorganización y desconocimiento del hombre sobre las cosas en un momento dado.

Diferentes tipos de archivos:

- Archivos públicos (aquellos manejados por el estado)
- Archivos privados (aquellos manejados por empresas privadas)
- Manuales (si son procesados en forma manual)
- Automáticos (si son procesados de modo automático)
- Sobre personas físicas (sean residentes o no de determinado pais.
- Personas morales.

Derecho a la protección de los datos personales, se trata de un derecho humano reconocido por el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, que impone obligaciones a las personas físicas o morales que utilizan datos personales, y que otorga derechos a los titulares de los datos, a fin de garantizar el buen uso de la información personal y la privacidad y derecho a la autodeterminación informativa de las personas.
La autodeterminación informativa no es otra cosa más que el derecho de las personas para decidir, de manera libre e informada, sobre el uso de la información que les pertenece.
Todo tratamiento o uso de datos personales conlleva un riesgo que, en caso de mal uso, gestión o cuidado, puede tener como consecuencia una intromisión ilegítima en la privacidad y la autodeterminación informativa de la persona que es titular de los datos personales. En ese sentido, al tratar datos personales se adquieren obligaciones para garantizar el debido tratamiento de la información.

Así pues, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

Dato personal, es cualquier información concerniente a una persona física identificada o identificable, como puede ser el nombre, los apellidos, la dirección postal, el número de teléfono, la dirección de correo electrónico, el número de pasaporte, una fotografía, la Clave Única de Registro de Población (CURP) o cualquier otra información que permita identificar o haga identificable al titular de los datos.
Los datos personales pueden estar expresados en forma numérica, alfabética, gráfica, fotográfica, acústica o en cualquier otra modalidad.
Se considera que una persona es identificable cuando su identidad puede determinarse mediante los datos personales de que se traten.
La información relativa a una persona moral no se considera como dato personal, quedando ésta excluida de la protección que otorga la normatividad sobre protección de datos personales a las personas físicas.
Es importante considerar que si los datos personales son objeto del procedimiento de disocian, de forma tal que no es posible asociarse a su titular, ni permitir su identificación, dejarán de ser considerados como tales y, por lo tanto, no será aplicable la normatividad sobre protección de datos personales.

Dato personal sensible, son datos personales que afectan la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen o conlleve un riesgo grave para éste, como, por ejemplo, el origen racial o étnico; estado de salud (pasado, presente y futuro); información genética; creencias religiosas, filosóficas y morales; afiliación sindical; opiniones políticas y preferencia sexual.

La protección de datos personales es un derecho humano que le da a los individuos el poder de controlar su información personal, decidir con quién se comparte y para qué se utiliza con terceros, así como el derecho a que ésta se trate

de forma adecuada, para permitir el ejercicio de otros derechos y evitar daños a su titular.

La Constitución Política, en su artículo 16, reconoce el derecho a la protección de datos personales como una garantía individual, al señalar que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de estos, así como a manifestar su oposición en los términos que fije la ley.

Tratamiento de datos personales, tratar datos personales es un concepto amplio, ya que incluye: Obtención, uso, divulgación y almacenamiento.
El uso de los datos personales abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.
Por ejemplo, un responsable del tratamiento puede obtener datos personales de una persona física, a través de un formulario en papel, almacenarlos en el disco duro de una máquina o en la nube, utilizarlos para sus actividades cotidianas, comunicarlos con el encargado que le brinda un servicio y suprimirlos cuando haya concluido la finalidad para la cual los obtuvo. Todas estas acciones se consideran tratamiento de datos personales.

Titular de los datos personales, Es la persona física a quien refieren y pertenecen los datos personales que son objeto de tratamiento. Por tanto, es el dueño de los datos personales, aunque éstos estén en posesión de un tercero para su tratamiento. Por ejemplo, el titular de los datos personales contenidos en un expediente laboral es el trabajador a quien refieren esos datos.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares establece las reglas, requisitos, condiciones y obligaciones mínimas que deberán observar los particulares que recaben, almacenen, difundan y utilicen datos personales. Esta Ley aplica tanto a los profesionistas o personas físicas que prestan sus servicios de manera independiente, entre ellos abogados, doctores o contadores, como a las organizaciones y micros, pequeñas, medianas y grandes empresas, como bancos, instituciones educativas, tiendas de autoservicio y departamentales, aseguradoras, asociaciones de profesionistas, clubes deportivos, entre otros.

Existen dos tipos de consentimiento:
1. Expreso. Es necesario cuando te soliciten datos personales sensibles, patrimoniales o financieros. Se manifiesta por escrito, verbalmente, por medios electrónicos o cualquier otro que permita demostrar de manera clara y patente que lo otorgaste.
2. Tácito. Se utiliza para el resto de los datos personales. No es necesaria una manifestación expresa de tu parte, sino que es suficiente que se haya hecho de tu conocimiento el aviso de privacidad y que no te hayas negado para el tratamiento de tus datos personales.

Para la obtención y uso de tus datos personales, los particulares están obligados a:

• Darles uso a los datos personales respetando la Ley, desde el momento de su obtención.
• No utilizar medios engañosos o fraudulentos para obtener los datos personales.
• Obtener tu consentimiento o autorización para el tratamiento de tus datos personales, salvo las excepciones previstas en el artículo 10 de la Ley.
• Darte a conocer el aviso de privacidad para que estés informado sobre quién y para qué recaba tus datos personales, cómo ejercer tus derechos ARCO, así como los términos y condiciones generales del tratamiento a los que será sometida tu información.
• Recabar sólo aquellos datos personales que sean necesarios para las finalidades para las que se obtienen.

Durante el tratamiento de tus datos personales:

• Sólo utilizar tus datos personales para las finalidades que autorizaste o consentiste.
• Mantener tus datos personales actualizados y correctos.
• Conservar tus datos personales sólo por el periodo que sea necesario para llevar a cabo la finalidad para la que se obtuvieron.
• Sólo compartir tus datos personales con terceros si lo autorizaste, salvo las excepciones previstas en el artículo 37 de la Ley.
• Guardar la confidencialidad de tus datos personales.
• Implementar medidas de seguridad que eviten el daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado de tus datos personales.
• Informarte si ha ocurrido una vulneración a la seguridad de las bases de datos que pueda afectar tus derechos patrimoniales o morales, para que puedas tomar las medidas que consideres necesarias en tu protección.

Una vez que ha concluido el uso de tus datos personales:

• Eliminar de las bases de datos o archivos tus datos personales.

Es importante que tengas presente que no siempre se podrán eliminar de manera inmediata tus datos personales, pues a veces será necesario conservarlos por algún periodo por cuestiones legales, de responsabilidades, o contractuales. A este periodo la Ley le denomina bloqueo, y durante el mismo tus datos personales no podrán ser utilizados para ninguna finalidad, y una vez concluido deberán ser eliminados.

El aviso de privacidad en el que te informen las características generales del uso de tus datos personales deberá contener entre otra la siguiente información:

1. Procedimiento para que se pueda revocar el consentimiento;
2. Datos personales recabados;

3. Señalamiento expreso de los datos personales sensibles que se usen;

4. Finalidades del uso de los datos personales;

5. Identidad y domicilio del responsable que recaba los datos personales;

6. Opciones para limitar el uso o divulgación de los datos personales;

7. Medios para el ejercicio de los derechos ARCO;

8. Comunicaciones a terceros de los datos personales;

9. Cláusula para que el titular indique si acepta o no la comunicación de sus datos personales, y

10. Procedimiento para comunicar los cambios en el aviso de privacidad.

La Ley otorga a los titulares de los datos personales el derecho a **acceder, rectificar y cancelar** su información personal en posesión de terceros, así como a **oponerse** a su uso. A estos se les conoce como **derechos ARCO**.

Derechos ARCO, derechos de acceso, rectificación, cancelación y oposición.

El objeto de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, es regular el tratamiento legítimo, controlado e informado de los datos personales, para garantizar así la privacidad de las personas y la protección de su información personal.

Los titulares de los datos personales tienen derecho de acceder a su información personal que esté en posesión de terceros, a fin de conocer cuál es y el estado en que se encuentra, es decir, si es correcta y actualizada, o para conocer para qué fines se utiliza. Asimismo, a través del ejercicio del derecho de acceso, se pueden conocer las características generales del uso al que están sometidos los datos personales. Entre la información a la que se puede acceder se encuentra la siguiente:

- ¿Cuáles de mis datos personales usan?
- ¿Para qué finalidades?
- ¿Quién utiliza mis datos personales?
- ¿Con quiénes comparten mi información personal y para qué fines?
- ¿Qué datos personales comparten con terceros?
- ¿De qué fuente obtuvieron mis datos personales?

Los titulares de los datos personales tienen derecho a rectificar su información personal, cuando ésta resulte ser incompleta o inexacta. En otras palabras, tú puedes solicitarle a quien utilice tus datos personales que los corrija cuando los mismos resulten ser incorrectos o desactualizados o inexactos.
A manera de ejemplo: cuando fuiste a abrir una cuenta de ahorros bancaria, el ejecutivo de cuenta registró, por error, un número de domicilio que no corresponde

con el tuyo, lo cual ha impedido que tus estados de cuenta lleguen a la dirección correcta. Ante esta inexactitud, tienes el derecho de acudir al banco y solicitar la rectificación respectiva, avalada por un comprobante de tu domicilio actual.

Los titulares de los datos personales pueden solicitar que se cancelen, es decir, se eliminen sus datos personales cuando consideren que no están siendo utilizados o tratados conforme a las obligaciones y deberes que tiene el responsable y que se encuentran contenidos tanto en la Ley como en su Reglamento.

Como se señaló anteriormente, la eliminación de los datos personales no siempre procede de manera inmediata, pues a veces es necesaria la conservación de estos con fines legales, de responsabilidades o contractuales. A este periodo la Ley le denomina **bloqueo**, y durante el mismo tus datos personales no podrán ser utilizados para ninguna finalidad, y una vez concluido deberán ser eliminados.
Por otra parte, es importante que tengas presente que no siempre procederá la cancelación de tu información personal. En particular, tus datos personales no podrán ser eliminados de una base de datos o archivo cuando:
• Se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento;
• Deban ser tratados por disposición legal;
• Se obstaculicen actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas;
• Sean necesarios para proteger los intereses jurídicamente tutelados del titular;
• Sean necesarios para realizar una acción en función del interés público;
• Sean necesarios para cumplir con una obligación legalmente adquirida por el titular, y
• Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto.
Un ejemplo de ejercicio del derecho de cancelación: cancelaste una tarjeta de crédito de una tienda de autoservicio hace 12 años, sin embargo, esta tienda te sigue enviando trimestralmente a tu correo electrónico una encuesta de calidad de sus servicios relacionados con la tarjeta de crédito. A través del ejercicio del derecho de cancelación, puedes solicitar a esta tienda que suprima o elimine tu información de sus registros, a efecto de que no recibas ninguna encuesta de calidad o cualquier otra información, debido a que ya no mantienes relación con la tienda de autoservicio, es decir, ya se agotó la finalidad para la cual obtuvieron y trataron tus datos.

Los titulares de los datos personales tienen derecho a oponerse al uso de su información personal o exigir el cese de este cuando:

• Por alguna causa legítima sea necesario parar el uso de los datos personales, a fin de evitar un daño a su persona.

• No quieran que su información personal sea utilizada para ciertos fines o por ciertas personas, empresas, negocios, asociaciones, o cualquier tercero.

Un ejemplo muy claro de este derecho es manifestar tu oposición al tratamiento de tus datos personales para fines comerciales o publicitarios. Imagina que compras un boleto de avión, y a partir de esa compra la línea aérea te envía cualquier tipo de promociones a tu correo electrónico. A partir del ejercicio del derecho de oposición, puedes solicitar a la línea aérea que no te envíe publicidad.

El responsable del tratamiento es la persona física o moral de carácter privado que decide sobre el tratamiento de los datos personales, es decir, la que establece las finalidades del tratamiento o el uso que se le dará a los datos personales, el tipo de datos que se requieren, a quién y para qué se comparten, cómo se obtienen, almacenan y suprimen los datos personales, y en qué casos se divulgarán, entre otros factores de decisión.
El responsable del tratamiento puede ser, por ejemplo, una empresa o persona moral, un emprendedor, un doctor, un abogado, un contador, una organización de la sociedad civil, una escuela o colegio, el patronato de un museo, una universidad privada o una fundación, o cualquier otra persona física o moral que decida sobre el tratamiento de los datos personales para el desarrollo de su actividad.

Encargado del tratamiento, es la persona física o moral, ajena a la organización del responsable del tratamiento, que trata los datos personales a nombre y por cuenta del responsable. A diferencia de este último, el encargado no decide sobre el tratamiento de los datos personales, sino que lo realiza siguiendo las instrucciones del responsable.

Por ejemplo, se considera encargado a la empresa que fue contratada por el responsable para administrar su nómina o prestarle el servicio de *call center*. También sería encargada del tratamiento una empresa que ofrece servicios de cómputo en la nube y que almacena bases de datos de un responsable, o bien, aquélla que contrató el responsable para la destrucción de sus documentos.
Si el encargado tratara los datos personales para finalidades propias, de forma tal que decidiera sobre dicho tratamiento, se convertiría en un responsable, con todas sus obligaciones, y estaría sujeto a las sanciones previstas por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en caso de incumplimiento.

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares aplica a todas las personas físicas o morales de carácter privado, que en el desarrollo de sus actividades traten datos personales, con excepción de los únicos dos supuestos previstos en su artículo:
1) Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y

2) Las personas físicas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

Entonces, sólo en los dos supuestos antes señalados no aplicará la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. En todos los demás casos en los que un particular trate datos personales aplicará la norma, por ejemplo, a los notarios, abogados, contadores, médicos, organizaciones de la sociedad civil, empresas, bancos, aseguradoras, escuelas, entre otros.

En ese sentido, tenemos que la Ley Federal de Protección de Datos Personales en Posesión de los Particulares además de no aplicar a las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia, ni a las personas físicas que traten datos personales para uso exclusivamente personal.

En suma, el artículo 2 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares establece excepciones a su aplicación para personas físicas y morales.

Ámbito de aplicación, la Ley y demás normatividad que derive de éstos, cuando no indique lo contrario, aplica al tratamiento de datos personales que obren tanto en soporte físico, como electrónico, siempre y cuando las bases de datos en las que estén contenidos hagan posible el acceso a los datos con base en criterios determinados, como podrían ser criterios específicos de búsqueda, nombre de los titulares, fechas, tipo de tratamiento, orden alfabético, o cualquier otro.
Lo anterior implica que si no es posible acceder a los datos con base en estos criterios y, por tanto, para ello se requieren plazos o actividades desproporcionadas, en esos casos, no aplicará la norma que regula la protección de los datos personales.
Por otra parte, para que la normativa en materia de datos personales aplique no es indispensable que los datos personales se encuentren en un formato en lo específico, ya que éstos pueden estar expresados en forma numérica, alfabética, gráfica, fotográfica, acústica o en cualquier otro tipo. Lo importante es que se trate de información concerniente a una persona física identificada o identificable.

Ámbito de aplicación territorial, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares es de observancia general en toda la República Mexicana, por lo que es la única ley que regula el tratamiento de datos personales en posesión de los particulares en el país. En ese sentido, no existen leyes locales para esta materia que apliquen al sector privado, con independencia de que las haya para regular el tratamiento de datos personales en posesión del sector público.
La Ley Federal de Protección de Datos Personales en Posesión de los Particulares aplica en cualquiera de los siguientes casos:
- El tratamiento de datos personales se realice en un establecimiento del responsable ubicado en territorio mexicano.

- El tratamiento lo realice un encargado a nombre de un responsable establecido en territorio mexicano, sin importar dónde se encuentre ubicado dicho encargado, ya que quien responde por el debido tratamiento de los datos personales es el responsable.
- El responsable no esté establecido en territorio mexicano, pero le resulte aplicable la legislación mexicana, derivado de la celebración de un contrato o en términos del derecho internacional.
- El responsable no esté establecido en territorio mexicano, pero utilice para el tratamiento medios situados en el país, salvo que tales medios se utilicen únicamente con fines de tránsito que no impliquen un tratamiento. En este caso, el responsable deberá proveer los medios necesarios para que los datos personales se traten conforme a la legislación mexicana, para lo cual, por ejemplo, podrá designar un representante en territorio nacional.

Asimismo, es importante señalar que cuando el responsable no se encuentre ubicado en territorio mexicano, pero el encargado lo esté, a este último le serán aplicables las disposiciones relativas a las medidas de seguridad previstas por la normativa en materia de protección de datos personales, así como el resto de las obligaciones que con relación al encargado establezca la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y demás normativa aplicable.

Transferencia de datos personales, se denomina transferencia de datos personales a la comunicación de datos que realiza el responsable del tratamiento a un tercero, distinto del titular, del mismo responsable (por ejemplo, las comunicaciones al interior de la organización del responsable, como las que se realizan entre el personal) o del encargado.

La comunicación puede producirse, entre otros actos, por el envío de los datos al tercero, por el hecho de mostrarlos en una pantalla o permitirle el acceso a los mismos.

La transferencia de datos personales puede ser nacional o internacional, según el destino de los datos personales. No obstante, en ambos casos, es necesario que se cumpla con todos los principios de la protección de datos, deberes y derechos que establece la norma mexicana.
Ejemplos de transferencias:
- Un patrón o una empresa (responsable del tratamiento) que comunica datos personales de sus trabajadores al Instituto Mexicano del Seguro Social (tercero), para el cálculo de la pensión.
- Una empresa del grupo corporativo A (responsable) comunica datos de sus clientes a otra empresa del mismo grupo (tercero), a fin de que esta última pueda ofrecer sus servicios.
- Un hospital (responsable) proporciona información de un paciente a la aseguradora de este último (tercero), a fin de que aplique el seguro de gastos médicos.

- Una universidad mexicana (responsable) envía datos personales de sus alumnos que van a participar en un programa de intercambio a una universidad de otro país (tercero).

Remisión de datos personales, al igual que en el caso de la transferencia, la remisión supone una comunicación de datos personales. La diferencia entre ambos conceptos consiste en que, en este caso, dicha comunicación se produce entre un responsable y un encargado del tratamiento.
Las remisiones también pueden ser nacionales o internacionales. Sin embargo, ambas están reguladas de la misma forma, como se verá más adelante, pues sin importar que el responsable del tratamiento remita los datos personales a un encargado dentro o fuera del territorio nacional, el primero sigue siendo quien responde por el debido tratamiento de la información personal que comunicó.
Ejemplos de remisiones:
- Una empresa comunica datos personales a un contador que le presta los servicios de elaboración de su nómina.
- Un banco comunica datos de contacto de sus clientes a un *call center* ubicado fuera del país, para que le preste el servicio de atención de quejas.
- Una institución financiera comunica datos personales a un despacho de cobranza para que le preste el servicio de cobranza extrajudicial.

Por delito informático, suele entenderse toda aquella conducta ilícita susceptible de ser sancionada por el derecho penal, consistente en el uso indebido de cualquier medio informático.

Organismos internacionales como la OCED, lo define como cualquier conducta, no ética o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos.

Para Julio Téllez Valdez, los delitos informáticos son aquellas actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico). El mismo autor establece como característica de dichos antijurídicos que son conductas delictivas de cuello blanco, porque se requieren conocimientos técnicos; son acciones ocupacionales por realizarse cuando el sujeto activo labora, y son acciones de oportunidad pues se aprovecha la ocasión o el universo de funciones y organizaciones de un sistema tecnológico y económico.

La Organización de las Naciones Unidas, reconoce como delitos informáticos las siguientes conductas:

1. Fraudes cometidos mediante manipulación de computadoras:
    a) Manipulación de los datos de entrada.
    b) Manipulación de programas.
    c) Manipulación de datos de salida.

d) Fraude efectuado por manipulación informática.
2. Falsificaciones informáticas
a) Utilizando sistemas informáticos como objetos.
b) Utilizando sistemas informáticos como instrumentos.
3. Daños o modificaciones de programas o datos computalizados.
a) Sabotaje informático.
b) Virus.
c) Gusanos.
d) Bomba lógica o cronológica.
e) Acceso no autorizado a sistemas o servicios.
f) Piratas informáticos o hackers.
g) Reproducción no autorizada de programas informáticos con protección legal.

En nuestro sistema jurídico se incluyó a los delitos informáticos justamente con las reformas que se publicaron en el Diario Oficial de la Federación el diecisiete de mayo de mil novecientos noventa y nueve.
Los novedosos ilícitos se ubicaron dentro de Título Noveno del código punitivo federal, al que se denominó “Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de Informática”.

Riesgos del Internet

1. Acceso a la información: El fácil acceso a una gran variedad de páginas, distrae al usuario de su objetivo inicial.

2. Tipos de información: Los usuarios pueden tener acceso a información inadecuada, agresiva, ilícita, pornográfica, entre otras.

3. Relaciones personales: Puede crear un entorno que facilita comportamientos desinhibidos y dar una imagen que no corresponde con la realidad. El uso excesivo puede generar un problema de socialización en las niñas, niños y jóvenes, ya que fomenta el aislamento.

4. Se puede producir una pérdida de intimidad: La participación en determinados foros, chats y redes sociales requieren que el usuario facilite datos personales a terceros o páginas falsas.

5. Amistades no convenientes: El uso de programas de mensajería instantánea y redes sociales permite el contacto con personas desconocidas, que pueden ser violentas y con intenciones ilícitas.

6. Adicciones: El uso excesivo de internet puede provocar “adicción”, sin embargo ésta dependerá de su perfil, circunstancias personales y situaciones de comportamientos compulsivos.

7. Relativos al propio funcionamiento de internet: Internet no es una red segura, ya que existen sitios web clonados y páginas con un gran número de spam y links de sitios webs que contienen información inapropiada.

8. Temas económicos: La facilidad para poder ingresar a sitios con miles de servicios y promociones falsas, pueden llevar a los usuarios a ser víctimas de engaños, fraudes, estafas, compras u negocios ilegales, etc.

Delito Cibernético, actos u omisiones que sancionan las leyes penales con relación al mal uso de los medios cibernéticos.

La Coordinación para la Prevención de Delitos Electrónicos de la Policía Federal impulsa el término “Delito Electrónico” en sustitución de “Delito Cibernético”, por ser un término más amplio que conjunta también los dispositivos como ipad, lap top, entre otros.

La facilidad para ingresar a los medios socio-digitales, incrementa los riesgos y comisión de conductas antisociales y/ o ilícitas que pueden alterar la integridad de los/as usuarios(as), como son los siguientes casos:

1. Conductas de riesgo
2. Conductas antisociales
3. Conductas Ilícitas.

Conductas de riesgo

Sexting es una palabra tomada del inglés que une “Sex” (sexo) y “Texting” (envío de mensajes de texto vía SMS desde teléfonos móviles). Sin embargo, el desarrollo de teléfonos móviles ha permitido que el término también englobe el envío de fotografías y videos.

Sus características principales son las siguientes:
- El/la protagonista posa en situación erótica o sexual.
- El material de texto, fotográfico o de video es producido de forma voluntaria por el mismo autor(a) quien lo difunde través del celular.

Relacionado con el sexting, existe otro fenómeno llamado **sex-casting** el cual se identifica por la grabación de contenidos sexuales a través de la webcam y la difusión de los mismos es por e-mail, redes sociales o cualquier canal que permitan las nuevas tecnologías.

Esta actividad no genera un daño en el momento de la producción a los autores(as), sin embargo, sí causa consecuencias negativas posteriores, como las siguientes:
- Amenazas a la privacidad del menor: cuando el material es visto por cualquier persona.
- Daño psicológico: cuando la difusión del material provoca que al autor se le someta a maltrato
y humillaciones, causando problemas de ansiedad, depresión, exclusión social o suicidio.
- Sextorsión: Cuando el material cae en manos de una persona que lo utiliza para extorsionar o chantajear al protagonista de las imágenes o videos.
- Riesgo de geolocalización: cuando las aplicaciones de geolocalización y geoetiquetado de contenido multimedia para dispositivos móviles pueden facilitar la ubicación física.

Ciberbullying, el acoso escolar (bullying) en medios electrónicos se conoce como ciberbullying.

El ciberbullying se da entre menores y se define como los insultos, humillaciones, amenazas, chantaje, entre otras ofensas a través de un dispositivo tecnológico.

Cibergrooming, consiste en el conjunto de estrategias que una persona adulta utiliza para ganarse la confianza de la o el menor a través de internet con el objetivo de conseguir concesiones de índole sexual, ya sea el envío de fotos o videos como de mantener un contacto físico.

Eric Stephens, director de tecnología de Microsoft México, describe los pasos que llevan a cabo este tipo de personas:

- Empatía: Crea empatía con la mayoría de las actividades que realiza la víctima, logrando que ella o él se sienta cómodo para obtener su confianza.
- Vínculo: Desarrolla intimidad con la/el menor de tal manera que lo convence de una amistad, de una relación de pareja o hermandad.
- Obtención de información: Sirviéndose del vínculo establecido, la/el ciber acosador rebasa los límites de la confianza, pidiendo información más comprometedora o reveladora, y sugiere que la/el menor realice acciones eróticas con partes de su cuerpo ante la webcam, las cuales servirán posteriormente para chantajearlo o forzarlo a citarse con el acosador en algún lugar.
- Intimidación: Obteniendo el primer material de video, fotográfico o escrito, la/el ciber-acosador amenaza a la víctima con la exposición del material a su círculo social, lo que va mermando emocional y psicológicamente a la víctima.
- Encuentro físico: Finalmente la/el ciber-acosador consigue encontrarse con su víctima20, para efectuar el ilícito.

Conductas antisociales

- Acceso a equipos “ajenos” sin autorización, con el fin de obtener beneficios en perjuicio de otro.
-Manipulación de información contenida en archivos o soportes físicos informáticos “ajenos”.
- Envío de programas maliciosos (malware) para la destrucción de datos, software, o el daño parcial del mismo equipo.

Conductas ilícitas derivadas del mal uso de internet:
• Uso de medios cibernéticos con fines fraudulentos.
• Robo y suplantación de identidades.
• Robo de información personal, bancaria, institucional o empresarial.
• Negociaciones de secuestros y extorsión.
• Pornografía Infantil.
• Trata de Personas.
• Narcomenudeo.
• Abuso sexual del/la menor.
• Maltrato infantil.
• Pederastia.

Contrato electrónico, la existencia de los contratos celebrados en Internet trae consigo cuestionamientos con respecto a la "desmaterialización" del proceso normal de contratar, así como el de cómo autentificar la capacidad de contratar de las partes y cómo apreciar la aceptación de una oferta realizada en Internet.

La Ley Modelo de UNCITRAL sobre comercio electrónico es un intento de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional de fomentar dicha armonización y unificación, con el interés del progreso amplio del comercio internacional, usando métodos de comunicación y almacenamiento de información sustitutos de los que usan papel. Su objetivo esencial es el de remediar los inconvenientes surgidos de los obstáculos derivados de los derechos nacionales que creen incertidumbre y limiten el acceso de las empresas a los mercados internacionales.

CARRASCO BLANC se refiere a la contratación electrónica señalando que se trata de “aquellos actos jurídicos bilaterales o convenciones que tienen por objeto crear; modificar o extinguir derechos (y su correlativa obligación) y que se celebran a través de medios de comunicación y/o medios informáticos”.

Contratos informáticos tienen por objeto específico ciertos bienes y servicios informáticos, por ejemplo, es un contrato de este tipo aquel mediante el cual se obtiene el acceso a una red.

La contratación electrónica se refiere a toda clase de contratos, cualquier sea su objeto, a condición de que se celebren mediante el empleo de medios electrónicos; así, por ejemplo, una compraventa, un seguro, un hospedaje, un pasaje aéreo, se

puede convenir por medios electrónicos y constituye contratación de esta naturaleza.

1. El contrato que se concluye en línea tiene la particularidad que la ejecución de su objeto se hace en el mundo material.
2. El contrato virtual también se concluye en línea, pero además su modo de ejecución es en forma electrónica

Elementos de existencia del contrato electrónico

Para la existencia del contrato se requiere:

I. Consentimiento;

II. Objeto que pueda ser materia del contrato.

Declaración de voluntad en la contratación electrónica

En el comercio electrónico se emplea como soporte para la expresión de la voluntad negocial generadora de obligaciones y derechos, el documento electrónico.

Para que el acto jurídico exista es necesaria la expresión de la voluntad, que cuando se trata de convenciones y contratos toma el nombre de consentimiento.

En el caso del comercio electrónico ha de tratarse de declaraciones de voluntad expresadas por medio de esta tecnología.

La expresión y la formación del consentimiento en la contratación electrónica tendrán que ajustarse en cierta medida a sus peculiaridades.

Cuando existe la manifestación de la voluntad de las partes de celebrar un contrato y el consentimiento es expresado libremente y sin vicios de la voluntad, ya sea por correo electrónico o por adhesión a un documento en el Web, este contrato existirá en nuestro país –dado el principio consensual de nuestro derecho contractual-, siempre y cuando no requiera de formalidades especiales señaladas por la ley.

Tratándose de aceptación electrónica, CARRASCO BLANC la define como “aquella declaración unilateral de voluntad que una persona realiza a través de medios de comunicación y/o medios informáticos manifestando su conformidad a una propuesta recibida por ella”.

La aceptación electrónica puede ser clasificada como expresa o tácita.

La aceptación debe cumplir ciertos requisitos de eficacia o de validez, a saber: debe darse mientras la oferta esté vigente, ha de ser oportuna y pura y simple.

-La firma electrónica tiene la misma validez que la firma autógrafa, los medios electrónicos (Internet) tienen la misma validez que la forma escrita, posibilidad de utilizar la fe pública notarial en forma electrónica.

Por regla general los contratos electrónicos celebrados vía Internet son contratos de adhesión, que impiden una negociación de las cláusulas en ellos contenidas.

Momento del perfeccionamiento, el contrato está perfeccionado desde el momento en que empieza a producir sus efectos, es decir, desde el instante en que las partes que lo han celebrado pueden hacer efectivos sus derechos y exigir el cumplimiento de las obligaciones que él ha generado.

La determinación del momento de perfeccionamiento del contrato depende si se ha celebrado entre partes que están presentes o entre contratantes que están ausentes. En el primer caso la cuestión no suscita dudas, porque ese instante tiene lugar cuando se forma el consentimiento, esto es, cuando se unen las voluntades de ambas partes, la de aquella que hace la oferta con la que da su aceptación, o cuando se entrega la cosa objeto del contrato o cuando se cumplen las formalidades que acompañan al consentimiento, respectivamente, dependiendo si el contrato es consensual, real o solemne.

La *aceptación* es el acto de admisión de una oferta, siendo esencial para la existencia del compromiso entre las partes. Con relación a sí la aceptación en Internet debe ser implícita o explícita, en general, la persona a la que se le hace la oferta no puede quedar obligada por su silencio, así que, si recibe un correo electrónico que le informa que no respondió a la oferta dentro de cierto periodo, no está obligado a responder. Puede ser implícita cuando ya existe un flujo regular de negocios entre las partes, las cuales tienen un uso ordinario de Internet como medio de comunicación y que han establecido una relación comercial permanente, basada en un contrato principal celebrado previamente, en el que se pacta esta forma virtual de realizar convenios.

La *oferta* en Internet implica necesariamente una declaración unilateral de voluntad por la cual la parte que la hace propone la celebración de un contrato a una o más partes, o al "público en general". Los efectos jurídicos de la oferta se dan independientemente de la aceptación, aunque la propuesta sin la determinación esencial y precisa de los elementos del contrato futuro no tendrá relevancia jurídica.

Salvo que el vendedor establezca en el documento electrónico que no está realizando una oferta (con expresiones como "sin compromiso", o "sujeto a confirmación"), la mayoría de los sistemas jurídicos europeos y de nuestros socios consideran que se hace una oferta de carácter mercantil y que su aceptación por el

comprador en Internet constituye un acuerdo de voluntades (contrato) que da lugar a la responsabilidad que las partes acepten.

La identidad de las partes en la contratación electrónica, uno de los problemas más complejos de la contratación electrónica es la seguridad, y una parte de ella radica en la identificación de los contratantes, tarea nada fácil de realizar a través de un medio de comunicación que no revela la identidad o que permite a los contratantes mantener el anonimato, si lo desean.

En la contratación tradicional es preciso emplear como elemento de identificación el nombre de los contratantes, norma que se establece en todos los ordenamientos jurídicos.

Creemos que no existiendo una prohibición expresa, a la ha de contratar por medios electrónicos (Internet), es necesario contar con un proveedor de servicio para acceder a ella, el cual exigirá una identificación y la verificará, en la generalidad de los casos. Una vez convenido el acceso a la red, el servidor asigna al usuario un código de cliente (login), una clave (password) y los códigos de acceso.

En el caso de que se celebre un contrato a través de Internet, se requerirán no sólo los nombres y apellidos de los contratantes, sino además su domicilio, región, país, código postal y correo electrónico, como elementos de individualización mínima. Por otra parte, cuando se contrata con un servidor el acceso a Internet, se otorga al usuario una dirección electrónica, la cual podría llevar su nombre.

Para dar una mayor seguridad, se ha creado la firma electrónica, que satisface las necesidades de identificación del autor de un mensaje de datos, de autenticidad e integridad del contenido del mismo y, más aún, se contempla asimismo la existencia de prestadores de servicios de certificación de firmas electrónicas.

El correo electrónico constituye la forma más usada en el comercio electrónico, permitiendo a las compañías establecer contacto directo con consumidores potenciales. Ya sea en una primera transmisión o después de un intercambio preliminar, este correo puede contener una oferta comercial. La persona a la que se hace la oferta lee la misma al consultar su buzón electrónico, teniendo esta oferta efectos desde el momento en que es leída por la persona a la que se dirige y después depende de la persona aceptarla o no, devolviendo un correo electrónico de aceptación a quien se la dirigió.

Principales problemas o retos de los contratos electrónicos

Jurídicos

- Manifestar la voluntad de manera expresa o tácita
- Perfeccionamiento

- Celebrar los contratos por escrito y firmarlos (formalidad)
- Posibilidad de probar la existencia de un contrato (su oferta y aceptación) mediante un medio electrónico

Tecnológicos

- Confidencialidad (privacidad)
- Autenticidad (¿quién envió el mensaje?)
- Integridad (mensaje no ha sido alterado)
- Fecha (de la oferta y aceptación)
- No Rechazo

Manifestación de Voluntad (Consentimiento)

Código Civil Federal (antes CCDF)

> Art. 1803 (antes): El consentimiento puede ser expreso o tácito. Es expreso cuando se manifiesta verbalmente, por escrito o por signos inequívocos…
>
> Art. 1803 (hoy): El consentimiento puede ser expreso o tácito,
> para ello se estará a lo siguiente:
> I.- Será expreso cuando la voluntad se manifiesta verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos, y
> II.- El tácito resultará de hechos o de actos que lo presupongan o que autoricen a presumirlo, excepto en los casos en que por ley o por convenio la voluntad deba manifestarse expresamente

Perfeccionamiento de los Contratos

- Primero es necesario distinguir entre el consentimiento entre presentes y entre ausentes
- Si los contratantes se encuentran forma en el momento en que el aceptante da su conformidad a la oferta que le hace el policitante, siempre y cuando la aceptación se haga inmediatamente y de manera lisa y llana.
- Si los contratantes se encuentran varios sistemas o momentos posibles para la formación del contrato.

Entre ausentes, según doctrina y legislación, en cualquier país puede(n) existir alguno(s) de los siguientes sistemas:

- Declaración (cuando el aceptante declara su conformidad con la oferta)
- Expedición (cuando el aceptante pone en el correo o envía {expide} la contestación afirmativa)
- Recepción (cuando el policitante recibe la aceptación, aunque no se haya enterado de su contenido)

- Información (hasta que el oferente se entera de la aceptación por el destinatario de la propuesta)

Regulación jurídica del flujo internacional de datos y de Internet

1.Flujo de Datos Transfronterizos

Según el Consejo Económico de la Organización de las Naciones Unidas, el flujo de datos transfronterizos (FDT) es la circulación de datos e información a través de las fronteras nacionales para su procesamiento, almacenamiento y recuperación.

2. Problemáticas Jurídicas Particulares

Implicaciones positivas

- Favorecimiento de la paz y la democracia
- Favorecimiento en el progreso técnico y el crecimiento
- Interdependencia económica de las naciones

Implicaciones negativas

- Vulnerabilidad social
- Amenaza a la identidad cultural
- Dependencia tecnológica exagerada
- Incidencia económica notoria

El flujo de datos transfronterizos trae aparejada las siguientes problemáticas jurídicas particulares:

1. Utilización ilícita de datos transmitidos al extranjero: El envío de información a otro país, en el estado actual de derecho, permite a aquélla escapar a la reglamentación a la que pudiera estar sometida en el país de origen. De aquí se pueden derivar atentados graves a las garantías de los ciudadanos o aun a la seguridad de los Estados, lo cual amerita sin duda una solución jurídica.

2. Tarifas y régimen fiscal aplicables: Si se ha reiterado el contenido económico de la información, es evidente que ésta deberá hallarse sujeta a una cotización económica y más aún si va a ser objeto de exportación, lo cual motiva en su caso un aumento o disminución de las tarifas por aplicar.

3. Atenta contra la soberanía de los estados: La teleinformática, al igual que otras manifestaciones tecnológicas, trae consigo una serie de repercusiones que en última instancia inciden en uno de los valores más importantes de toda nación: su

soberanía, lo cual implica tener un control jurídico que evite o al menos limite este tipo de situaciones.

4. Revestimientos contractuales en torno a la información: Como un verdadero bien que puede ser objeto de derechos y obligaciones y por tanto materia del contrato en sus diferentes modalidades, motiva una reducción particular de cláusulas afines a su naturaleza que prevean posibles conflictos generados por dichos convenios, así como los riesgos a que pueda estar sometida y su eventual aseguramiento.

5. Propiedad intelectual de la información: Es decir, los problemas que pudieran suscitarse en cuanto a la disputa o reivindicación de la propiedad intelectual de la información respecto a la disponibilidad y, por ende, probables beneficios económicos que ello genere, sobre todo por la amplia cobertura o difusión que pudiera tener a través de las redes teleinformáticas.

6. Seguridad jurídica de las empresas teleinformáticas: Esa información o redes pueden ser motivo de ilícitos ya sea como medios o como objetivos, por lo que una contemplación internacional en términos penales limitaría dichas acciones en forma no sólo correctiva, sino también preventiva.

- Autonomía de las ramas del derecho
- Comercio electrónico, sus fuentes de regulación, sujetos.
- Gobierno electrónico
- Transparencia
- Acceso a la información
- Protección de datos personales
- Información
- Dato
- Derecho al olvido
- Derecho a la desconexión
- Teletrabajo
- Derechos Humanos de Cuarta Generación
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados