TÓPICOS DE DERECHO INFORMÁTICO

Marco Antonio Besares Escobar

La sociedad de la información tiene uno de sus pilares en la aparición y posteriormente la utilización cada vez más cotidiana de las nuevas TIC, éstas han cambiado la forma en la que los humanos se relacionan unos con otros y por supuesto han generado diversos tipos de interacción entre las personas y la tecnología.

El presente libro aborda diversos temas relacionados con el derecho informático y la informática jurídica; temas que cada vez son de mayor relevancia y que con frecuencia son relegados de los estudios jurídicos.

Tópicos de Derecho Informático se encarga de analizar, interpretar y desentrañar algunas de las relaciones resultantes del binomio humano-tecnología, vistas desde la óptica de un jurista que en su ocupación ha hecho uso cotidiano de ellas.

UNACH | INSTITUTO DE INVESTIGACIONES JURÍDICAS

ISBN: 978-0-9862237-2-3

TÓPICOS DE DERECHO INFORMÁTICO

Marco Antonio Besares Escobar

UNACH | INSTITUTO DE INVESTIGACIONES JURÍDICAS

TÓPICOS DE DERECHO INFORMÁTICO

UNACH | INSTITUTO DE INVESTIGACIONES JURÍDICAS
CARLOS EUGENIO RUIZ HERNÁNDEZ, RECTOR

ISBN: 978-0-9862237-2-3
Editado en Austin, Texas; 2015

Universidad Autónoma de Chiapas

Instituto de Investigaciones Jurídicas

Ocozocoautla, Chiapas
7 de octubre de 2015
Memorandum No. CE/IIJ/01/15

Dr. Carlos F. Natarén Nandayapa
Encargado de la Dirección General
Instituto de Investigaciones Jurídicas
Presente

Por este medio comunicamos a usted que con fecha 5 de octubre del presente año, el Consejo Editorial del Instituto de Investigaciones Jurídicas en su 1ª sesión ordinaria acordó autorizar la publicación de la obra **"TÓPICOS DE DERECHO INFORMÁTICO"**.

Cabe mencionar que se ha constatado que los artículos que integran dicha obra cumplen con lo dispuesto en el Reglamento Editorial del Instituto de Investigaciones Jurídicas

Atentamente
"Por la conciencia de la necesidad de servir"

Dr. Oswaldo Chacón Rojas
Presidente del Consejo Editorial

Mtra. Adriana Yolanda Flores Castillo
Secretaria del Consejo Editorial

Mtro. Omar David Jiménez Ojeda
Vocal

ÍNDICE

PRESENTACIÓN

El presente libro aborda diversos temas relacionados con el derecho informático y la informática jurídica; temas que cada vez son de mayor relevancia y que con frecuencia son relegados de los estudios jurídicos. En su tratamiento, el autor, un jurista chiapaneco, hace evidente su experiencia como servidor público y como notario, además de su historial como académico de reconocido prestigio.

Este trabajo de investigación es un reflejo de los esfuerzos que la Universidad Autónoma de Chiapas realiza para establecer un Centro de Investigación en Derecho que aporte estudios jurídicos serios y metodologicamente rigurosos, que elaborados desde la perspectiva de las entidades federativas, contribuyan con soluciones a problemas sociales concretos, difundan los derechos de las ciudadanas y los ciudadanos dentro del Estado de Derecho y apoyen en el proceso de elevar el nivel académico de corte jurídico en nuestra región.

Por lo anterior, esta obra resulta una consecuencia necesaria al considerar el desarrollo tecnológico actual, ya que en el uso de las nuevas Tecnologías de la Información y Comunicación (comúnmente llamadas TIC) es normal que surjan problemas y que varios de ellos se relacionen con el derecho, por lo que el jurista y el investigador jurídico no pueden quedar ajenos.

La sociedad de la información tiene uno de sus pilares en la aparición y posteriormente la utilización cada vez más cotidiana de las nuevas TIC, éstas han cambiado la forma en la que los humanos se relacionan unos con otros y por supuesto han generado diversos tipos de interacción entre las personas y la tecnología.

El doctor Marco Antonio Besares Escobar ha demostrado desde hace varios años su preocupación por estos temas jurídicos; en el presente libro se encarga de analizar, interpretar y desentrañar algunas de las relaciones resultantes del binomio humano-tecnología, vistas desde la óptica de un jurista que en su ocupación ha hecho uso cotidiano de ellas.

En la obra pueden identificarse varios temas, el primero de ellos se dirige hacia la relación entre el derecho penal y las nuevas tecnologías. En efecto, la dinámica entre el ser humano y la tecnología ha traído avances significativos, sin embargo a la par de estos avances también han surgido espacios problemáticos en torno a su uso, tan es así que dentro del derecho informático encontramos una disciplina especial di-

rigida al estudio de las conductas delictivas relacionadas con el uso de las TIC o bien dentro de un ambiente virtual.

De esta manera, el autor nos lleva por un recorrido por los delitos en contra de la seguridad informática, los cuales se relacionan directamente con el derecho a la intimidad.

En esta tesitura, las TIC se han convertido en herramientas para concretar delitos, pero también en el ambiente virtual existen diversas conductas que son catalogadas de la misma forma, por ello, el derecho penal informático o derecho penal de las nuevas tecnologías de la información y comunicación se encarga de su estudio. El autor retoma el estudio de estos delitos a través del análisis particular de sus elementos, lo cual es muy útil tanto para el estudiante de derecho, el investigador, como para el juzgador, incluso para el litigante.

Otra de las partes de esta obra se dedica al estudio de la seguridad informática en la función notarial. La experiencia del autor como Notario Público se traduce en una gran facilidad para comentar estos temas, que no son menores en la labor del notario, pues de ello depende desde el cálculo de impuestos hasta el alta de avisos a diversas plataformas gubernamentales, en donde la seguridad de los datos personales (incluidos datos bancarios) es prioritaria.

Por otra parte, uno de los insumos de esta sociedad de la información es precisamente esta última: la información, que se ha convertido en una fuente de poder, quien tiene la información tiene el poder. Por ello, es imperante que las

leyes que garantizan el derecho de acceso a la información pública y la transparencia gubernamental cumplan con diversos criterios para cumplir con esta encomienda.

En esta inteligencia, parte de la obra se dedica a la revisión de la legislación estatal aplicable al derecho de acceso a la información y a la transparencia gubernamental, a través del estudio de sus elementos, algunos puntos de derecho comparado y distintas observaciones sobre las luces y sombras que se encuentran dicho ordenamiento legal.

Finalmente, la contratación electrónica no es para nada algo ajeno a nuestra vida cotidiana, tanto inmigrantes como nativos digitales hacen uso de esta herramienta sin reparar en los elementos que la conforman y los alcances que este tipo de contratación puede tener. En este sentido, este libro propone el estudio de los componentes de la contratación electrónica así como el estudio de los ordenamientos legales que conforman el marco jurídico nacional y un ejercicio de derecho comparado con el derecho español.

Este tópico es importante en el estudio de las relaciones jurídicas, pues es difícil discernir si existe una expresión del consentimiento, qué legislación resulta aplicable cuando se trata de páginas domiciliadas en otros países, entre otras complicaciones; por ello contar con una referencia tanto teórica como práctica resulta por demás útil para los operadores jurídicos.

En resumen, esta obra que nace del pensamiento de un jurista chiapaneco dentro del grupo de investigadores

del IIJ-UNACH, se erige desde ahora como una de las principales referencias en los temas relacionados con el derecho informático, esperando que el análisis y las propuestas generadas tengan eco en la sociedad chiapaneca.

Carlos F. Natarén Nandayapa
Director

DELITOS CONTRA LA SEGURIDAD INFORMATICA Y EL DERECHO A LA INTIMIDAD EN MÉXICO

1.- INTRODUCCIÓN

Cada país ajusta su sistema jurídico de acuerdo a su nivel de organización política y social, así como las directrices de su política internacional, en México ocurre igual. Ante el proceso acelerado de cambios sociales derivados del desarrollo de las tecnologías de la informática y las comunicaciones, las relaciones sociales, los nuevos roles[1] y su regulación en el ámbito jurídico tienen un ritmo diferente de evolución, el derecho por su carácter estricto y formal, reacciona a una velocidad menor[2], no obstante ya existe un número signifi-

[1]Su uso ha producido nuevas relaciones sociales entre los actores, usuarios, proveedores y propietarios de la información.

[2]El reto principal de los sistemas jurídicos penales nacionales es el retraso existente entre el avance tecnológico y la aparición de la conductas tipificadas en el derecho. La sugerencia de los pasos para la evolución jurídica nacional pueden consultarse en Ciberdelitos. "Una guía para los países en vías de desarrollo". Versión digital. www.

cativo de normas, propicias para el análisis político criminal y dogmático.

En el contexto de la Sociedad de la Información o como la llaman otros, la TecnoEra, caracterizada por el dinamismo de las tecnologías de la información y la comunicación y la masiva producción de información a velocidades y cantidades inusitadas, surgen nuevas formas de convivencia entre los integrantes de una nación y los de la aldea internacional, trayendo consigo una serie de conductas ilícitas relacionadas con el uso de estas tecnologías, así como nuevos bienes que proteger tanto por el derecho en general como por el derecho penal en particular.

Las consecuencias lesivas de estas conductas han provocado, que mediante el control social de reacción de los estados nacionales, se tomen decisiones de política criminal con pretensiones globales[3], que se reflejan en una serie de actos internacionales sobre la relación del derecho con este desarrollo tecnológico; tanto así que se reconoce la existencia del Derecho Informático como una nueva área de estudio jurídico. En el caso específico del derecho penal y las tecnologías de la información y la comunicación (TICS), ha surgido la especialización del Derecho Penal Informático,

---

itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf

[3]La Agenda sobre Ciberseguridad Global (GCA) de mayo del 2007, plantea cinco áreas estrategias de intervención, 1.- Medidas legales; 2.- Medidas técnicas y de procedimientos, 3.- Estructuras institucionales, 4.- Creación de capacidades y 5.- Cooperación internacional.

que se ocupa de analizar dichas conductas, denominándolas, delitos cibernéticos o ciberdelitos, electrónicos, telemáticos, digitales, informáticos y computacionales, entre otras denominaciones.

Esta múltiple denominación denota la complejidad del análisis jurídico penal en la materia, dada principalmente por el carácter técnico y terminología del lenguaje cibernético, lo que plantea un nuevo reto político criminal, ya que es una de las áreas emergentes del derecho que se enfila, con gran vigor, a sumarse al proceso de expansión[4] del derecho penal. (Puig, 2003). Esta tendencia se fortalece por la consideración sociológica de las características de la denominada sociedad del riesgo, en la medida en que la incorporación de las TICS a la vida de las personas depende de la eficacia[5] y

[4]Sobre este tema el penalista peruano Luis Reyna Alfaro, en un trabajo específico sobre la victima informática advierte sobre los peligros de la expansión del derecho penal con la emergencia de los delitos informáticos y dice. "La criminalización de los delitos informáticos aparece así dentro del proceso de expansión del Derecho penal, caracterizado por la inflación de ésta rama del ordenamiento jurídico. En *la Criminalidad Informática como manifestaci*ón de la *Sociedad del Riesgo*.:" de la " Riesgo.. ... víctima

[5]Elky Villegas Paiva sostiene en "Los bienes jurídicos colectivos en el derecho penal. Consideraciones sobre el fundamento y validez de la protección penal de los intereses macrosociales" que la noción de acudir al Derecho penal para contrarrestar los nuevos riesgos ocasionados por el hombre para evitar la lesión o puesta en peligro de intereses vitales para la sociedad, se basa también en el entendimiento de que el desarrollo científico y tecnológico, el afianzamiento de los medios de comunicación y la integración de los mercados, dan origen a nuevas formas de criminalidad, más sofisticada, ajustada en palabras de Pariona Arana a estos nuevos tiempos, una criminalidad que hace uso de la tecnología, conocimientos científicos y modernas formas de organización. Así tenemos una criminalidad organizada, una criminalidad informática, una criminalidad cometida al amparo del ejercicio del poder, una criminalidad económica, entre otras formas de manifestación.

el buen desarrollo de los sistemas y equipos de informática, lo que no sólo planteará la protección penal en los casos de daño a estos bienes, sino además en aquellos en que se ponga en riesgo la adecuada funcionalidad del ambiente informático de la sociedad.

La clasificación internacional del fenómeno de la cibercriminalidad y su recepción específica en cada país,[6] provoca una serie de problemas en su instrumentación, lo que impone la necesidad de hacer un ejercicio de interpretación dogmática con rigor sistemático del marco jurídico de cada Estado.

En nuestro caso, conviene hacer el análisis respecto del contenido del Código Penal Federal, que a partir del 17 de mayo de 1999 incorporó una serie de tipos penales, además del capítulo penal de la Ley Federal de Protección de Datos personales en posesión de particulares, que mantienen una estructura en cierta medida alineada a los criterios político criminales internacionales de la materia, enfocados en gran medida a la protección de la seguridad. Abordaremos también los Delitos Informáticos en materia federal, tanto los particulares del Código Penal, como los delitos federales especiales de la mencionada ley de datos personales, en cuanto a la legislación estatal haremos referencia única-

[6]Lara Martínez, señala que en el caso de Chile, siguiendo la subclasificción de la ONU regulada en la Ley 19223, los delitos de Sabotaje informático y el espionaje informática son equivalentes a las figuras típicas reguladas en el capítulo segundo del Título Noveno del Código Penal Mexicano.

mente a la correspondiente al Estado de Chiapas, todos los casos por supuesto están sujetos a la tendencia de armonización internacional.

Con el presente ensayo pretendemos contribuir a este debate y al avance del ejercicio analítico en este campo que también plantea retos metodológicos, ya que podemos anticipar, que en muchos casos no será sencillo resolverlos con las fórmulas o modelos tradicionales, toda vez que estos se inscriben en los denominados delitos económicos de las posmodernidad y son atendidos desde otros principios y criterios.[7]

Respecto a la literatura jurídica nacional en la materia, advertimos que una parte de lo publicado ha tenido limitaciones; algunos textos no logran agotar y profundizar el análisis del objeto de estudio por su amplia dimensión y su complejidad técnica, otros por la falta de delimitación y algunos otros porque los autores adolecen de una cultura informática suficiente. En el campo de la dogmática penal han surgido una serie de textos[8] que hacen un modesto esfuerzo y aplican los modelos tradicionales para el examen de estas figuras típicas.

Haremos pues, el desglose dogmático de los tipos penales que se encuentran en la mencionada legislación; ana-

---

[7]Ver sobre el tema de la inconveniencia de la aplicación de los modelos tradicionales a los delitos informáticos Graciela M. Landa Duran. Los Delitos informáticos en España y México. www.ijf.cjf.gob.mx/publicaciones/revista/24/r24_9.

[8]Ver el contenido del libro de Alberto Enrique Nava Garcés. Análisis de los delitos informáticos. Editorial Porrua. México. 2005.

lizando sus elementos y problemática, con el fin de auxiliar a los que lo requieran para la interpretación y aplicación en casos concretos de la operación jurisdiccional.

2.- CONTROL SOCIAL Y POLÍTICA CRIMINAL INFORMÁTICA

Para contextualizar el estudio específico y sistemático de los tipos penales informáticos de la legislación penal federal mexicana y de nuestra entidad federativa, hay que considerar los conceptos de control social[9] y política criminal.

El penalista español Francisco Muñoz Conde (1999) sostiene que:

> El control social es una condición básica de la vida social, con él se aseguran el cumplimiento de las expectativas de conducta y los intereses contenidos en las normas que rigen la convivencia, confirmándolas y estabilizándolas contra fácticamente, en caso de su frustración o incumplimiento, con la respectiva sanción impuesta en una determinada forma o procedimiento. El control social determina, pues, los límites de la libertad humana en la sociedad, constituyendo, al mismo tiempo, un instrumento de socialización de sus miembros.

[9]Las raíces del concepto de control social pueden encontrarse en las ideas de Platón y Aristóteles. Todas las escuelas sociológicas están de acuerdo en que para la existencia de la sociedad es necesario un grado mínimo de solidaridad, y que en ella impere cierto orden social, premisa de una sociedad moderna.

Se entiende pues, que el Control social es la capacidad de una sociedad para regularse de acuerdo a principios y valores consensuados, éste tiene dos propósitos: regular la conducta individual y mantener la cohesión social. Se dirige a los individuos con la finalidad de asimilar en ellos los valores aceptados por el grupo, para mantener el orden social necesario y funcional para la existencia de las estructuras del Estado, el cual a su vez reproduce las condiciones para la armónica convivencia social.

En este sentido, existe una importante corriente ideológica del *control social informal*, que contempla la posibilidad de inducir un comportamiento ético y jurídico en el ámbito de la sociedad de la información mediante una serie de acuerdos entre los sujetos para regular gran parte de los comportamientos de los usuarios de las tecnologías y navegantes de la red; sin embargo, por otra parte en el *control social de reacción*, respondiendo a una tendencia de estandarización internacional,[10] se han clasificado una serie de conductas consideradas para ser tratadas por el ejercicio del

[10]Díaz Gómez (2010), sostiene "La globalización y las transformaciones económicas que la explican han hecho posible la aparición, desarrollo y masificación de las nuevas tecnologías de la información. Paralelamente, el desarrollo tecnológico ha traído de la mano nuevas formas delictuales que tienen por medio o finalidad los sistemas informáticos e Internet. Las peculiaridades de estos nuevos tipos exigen un tratamiento conjunto y coherente, y del mismo modo, su problemática particular involucra a elementos transnacionales, lo que obliga a la utilización de la cooperación internacional para la adopción de medidas globales. Mediante esta técnica es posible lograr una armonización del Derecho sustantivo, así como en el ámbito procesal, que redunda definitivamente en un alivio de la singular incertidumbre que rodea los tipos ciberdelictuales".

poder punitivo del Estado, sobretodo desde la perspectiva de la seguridad informática.

El profesor alemán Heinz Zipf (1979), indica:

> La política criminal es un sector objetivamente delimitado de la política jurídica general: es la política jurídica en el ámbito criminal. En consecuencia, la política criminal se refiere a la determinación del cometido y función de la justicia criminal, consecución de un determinado modelo de regulación en este campo y decisión sobre el mismo (decisión fundamental político criminal) su configuración y realización de prácticas en virtud de la función, y su constante revisión en orden a las posibilidades de mejora (realización de la concepción política criminal).

Definición importante ya que reconoce el papel crucial que representa esta disciplina en la construcción de la estructura jurídico penal de una sociedad determinada. Para los propósitos de nuestro análisis, permite concluir sobre el modelo de regulación de delitos informáticos en México y su correspondencia con otros modelos de otros estados nacionales y con los criterios de los organismos internacionales que dirigen la política internacional.

Por ello, considerando que la *política criminal* es uno de los instrumentos de control social formal que cobra realidad en el derecho penal material y retomando la idea del profesor Juan Bustos (1997): "la Política Criminal es aquel aspecto del control social que tiene relación con el poder del Estado Nacional para caracterizar el conflicto social como criminal",

podemos decir que el Estado Mexicano, ha criminalizado una serie de comportamientos al incorporarlos a su legislación federal y estatal observando lineamientos internacionales. "Esto desde luego, contribuye al fenómeno de expansión del derecho penal, que cada vez más acelera la tendencia de ampliar el catalogo de delitos, ya que no tiene aparejada la descriminalización de otras conductas de bagatela como debiera ser en una sociedad organizada bajo los principios de un Estado Social y Democrático de Derecho." (2014).

Para ahondar en este aspecto, vale comentar que en esta etapa de desarrollo de la sociedad capitalista global, en donde las expresiones nacionales han cedido espacio a las decisiones supranacionales, el concepto delimitado a la política criminal aplicada en un país, va armonizándose, estandarizándose o uniformándose a principios rectores de política criminales de carácter global.

Durante la primera convención sobre el crimen cibernético realizada en Europa se planteó la necesidad de obtener respuestas homogéneas y precisas ante el aumento de la criminalidad cibernética, a lo que siguieron una serie de acciones a nivel global agrupadas dentro del lema "cibercriminalidad: un desafió global, una respuesta universal."[11]

[11]Lema de las Jornadas que durante dos días 12 y 13 de diciembre 2005, se desarrollaron en Madrid con el fin de que los países de la Organización de Estados Americanos (OEA) se sumaran al Convenio contra el Ciberdelito impulsado por la UE, que ha sido suscrito por naciones como EEUU, Japón, Sudáfrica y Canadá, declaró el representante europeo Guy de Vel. http://www.infobae.com/2005/12/11/227779-el-ciberdelito-es-motivo-analisis-europa

Existen opiniones que sostienen que es necesario instrumentar una política criminal alternativa reduccionista, tanto en el plano internacional como en el nacional, que contemple a los auténticos responsables que afectan bienes jurídicos relacionados con las tecnologías de la información y la comunicación, reorientando o desplazando su interés a otros agentes o actores criminales todavía no contemplados de manera adecuada por los procesos de criminalización, como es el caso de la grandes corporaciones u organizaciones criminales que incurren en *cibercriminalidad*, por ejemplo elaborando virus para después ofrecer el remedio cibernético con las famosas vacunas y disminuyendo el catálogo de delitos previstos para los sujetos individuales y dando intervención a otros ámbitos del derecho (Barata, 1977).

En este sentido, cabría plantearse cuáles son los conflictos derivados del uso de las nuevas tecnologías de la información que requieren ser atendidos por la política criminal del Estado mexicano y su congruencia de estandarización internacional para enfocar los esfuerzos hacia los responsables de la afectación de los valores o intereses jurídicos protegidos en la materia.

En este estudio nos interesa la política criminal desarrollada a partir del surgimiento de conductas ilícitas derivadas del uso de los sistemas informáticos y la orientación de la reacción punitiva que el Estado mexicano formula en torno a ellas; es necesario precisar entonces, que tanto el concepto de *política criminal* como el de *política criminal informática* se

refieren, en este caso, a la *política* en el sentido de conjunto de directrices, prácticas y normas que emanan de uno o de varios actores públicos que corresponden a una versión de las políticas públicas "entendidas como programas de acción gubernamental en un sector de la sociedad o en un escenario geográfico[12] con un contenido, orientación normativa, factores de coerción y una competencia social". Así tendremos que la política criminal legislativa en México tiene dos niveles concretos, el de la jurisdicción federal y el de las entidades federativas; en ambos niveles existen expresiones concretas de tipificación de delitos informáticos.

La incorporación de los delitos informáticos a la legislación nacional, responde en cierta medida, a la clasificación de los delitos cibernéticos propuestos por diversos instrumentos internacionales que tienen particular preocupación de proteger los bienes jurídicos afectados por conductas ilícitas producto del mal uso de sistemas y medios informáticos y de la comunicación, y es obvio que el origen de esta normatividad penal no ha surgido como respuesta de una problemática que considere las prioridades nacionales, sino como respuesta a la gran interacción internacional a través de una economía que se desarrolla en un escenario cada vez más virtual, basta revisar la tendencia de crecimiento del comercio electrónico o del mundo financiero y demás suce-

[12]En el caso de la política criminal informática tendríamos que abandonar el concepto original de lo que es un escenario geográfico, ya que el desarrollo de los medios informáticos nos obliga hablar de un nuevo plano, el ciberespacio.

sos del mundo virtual que construyen un derecho orientado a generar seguridad.

La política criminal se manifiesta en una serie de instrumentos y no sólo se basa en medidas jurídico – penales, estos instrumentos se relacionan entre si para evitar que se realice el delito o se produzca su reiteración; por ello el derecho penal corresponde a una clara expresión de la política criminal dentro de la línea general de política del estado; sin embargo, el derecho penal no es el único instrumento en el que se basa la política criminal para la solución de los problemas, sino también plantea medidas preventivas para el tratamiento de la criminalidad,[13] como lo es la política preventiva de los delitos informáticos, con las acciones de la policía cibernética o informática en diversos países, o como la promoción de un comportamiento autorregulado en el ámbito del uso de las nuevas tecnologías con la convención de códigos éticos.

[13]Moisés Moreno Hernández (1998), sostiene que "Al ser el derecho penal un instrumento político-criminal del Estado, puede revestir diversas características, según sea concebido y utilizado por el propio Estado, éste le puede imprimir las características que desee, de suerte que puede colocarlo en los extremos de un sistema penal democrático o en los de un sistema penal autoritario, o bien lograr un punto intermedio. El derecho penal, en todo caso, cualesquiera que sean sus rasgos característicos, será un indicador importante para definir el conjunto estatal, es decir, al Estado, como un Estado democrático o como un Estado autoritario, independientemente de otros indicadores."

3.- PRINCIPIOS DE POLÍTICA CRIMINAL Y DELITOS INFORMÁTICOS

Con el propósito de establecer criterios generales de análisis del tema, definimos los principios que orientan la política criminal del Estado Mexicano, y sólo para los efectos de la presente exposición, nos referimos a los principios de ultima ratio, legalidad y culpabilidad, que se relacionan con algunos de los problemas presentes dentro de la gestión para el uso de sistemas informáticos.

3.1. Principio de ultima ratio

El principio de intervención mínima del derecho penal se debe de observar en el derecho penal informático, ya que la criminalización de las conductas se debe dar en los casos más graves y por la naturaleza e importancia de los bienes informáticos y sólo cuando no permiten un tratamiento distinto al penal, es decir cuando es la solución de última instancia, esto es cuando otros métodos hallan fallado en su propósito de evitar las conductas no deseadas, sin perjuicio de la concurrencia de otras normas del ordenamiento jurídico, en estos supuestos cuando haya que proteger derechos humanos vinculados a este nuevo entorno cibernético.

En algunos países democráticos en los últimos años, para contrarrestar la expansión del derecho penal se ha dado

la tendencia hacia la despenalización de algunas conductas delictivas, desplazando su regulación a otras disciplinas distintas al derecho penal (tal es el caso del derecho civil y administrativo); sin embargo, en el panorama mundial ocurre lo contrario respecto al derecho informático, ya que la incorporación de supuestos delictivos tanto de delitos informáticos como de los denominados computacionales incrementan el catálogo de delitos de la legislación punitiva. Por ello, es esencial encontrar las fronteras racionales entre del derecho penal informático y el derecho administrativo sancionador de las conductas que afectan intereses y valores en las relaciones sociales que se manifiestan en este entorno.

En este sentido, recientemente se han realizado una serie de convenciones para abordar la problemática originada por los delitos informáticos. La comunidad internacional se encuentra preocupada por los intereses en juego frente a estas nuevas conductas delictivas (intereses de carácter económico, comercial, moral, seguridad, financieros, de intimidad o privacidad, etc.), por lo que ha decidido reaccionar acrecentando, desafortunadamente, la intervención del derecho penal.

Al respecto, en una postura que compartimos ante el riesgo del incremento de uso de la facultad punitiva del estado justificada por el fenómeno informático, Eugenio Raúl Zaffaroni (1994), argumenta:

> Resta una respuesta: ¿qué pasa con los grandes problemas? ¿Qué pasará con todos los problemas que hoy se pretende que resuelva el derecho penal? Simplemente, el derecho pe-

> nal no los resolverá, porque no puede resolverlos, porque no los está resolviendo ni los podrá resolver jamás. Los grandes problemas (medio ambiente, economía transnacional, armamentismo, consumo de drogas, etc.) deberán resolverse. La coacción jurídica como intervención o coacción directa será necesaria en muchas oportunidades, pero eso no es ni será jamás derecho penal. El derecho penal dejará de vender ilusiones, de convertirse en el sencillo expediente de los organismos políticos para que éstos aumenten su clientela demagógicamente creando la apariencia de soluciones, cuando sólo crean papeles que tienen el doble efecto de ocultar los problemas y despreocuparse por la búsqueda de soluciones reales, haciendo recaer el poder que a partir de ellos aumenta su arbitrariedad sobre los más desprotegidos y carentes del planeta; en nuestro caso, los más pobres de las sociedades pobres. Los penalistas deben de aprender a enseñar a las sociedades que ningún problema demasiado grave puede dejarse en sus manos.

Ahora bien, respecto del tema de la criminalidad organizada informática y de las graves afectaciones a los derechos humanos en esta materia, no confiamos en la función subsidiaria de la sanción penal, con relación a otras formas de sanción no penal ya que por su carácter aflictivo, la pena tiene una carga de reproche jurídico que, por ejemplo, las sanciones civiles o administrativas no podrían expresar. Permitir que los casos más graves cometidos, principalmente, por agentes dotados de poder económico, como el caso de las corporaciones y sus integrantes, se resuelvan espontáneamente mediante mecanismos de negociación o de

reserva del procedimiento administrativo, de acuerdo a las reglas del mercado, es particularmente delicado.

Finalmente, De la Cuesta Aguado (1999) en una posición también interesante, observando la teoría de la complejidad y rescatando el concepto de *estado crítico* sostiene:

> El derecho penal mínimo, es decir, aquél que sólo debe intervenir cuando sea imprescindible para que la violencia informal no supere la violencia formal ejercida por el propio sistema penal, debe permitir a la sociedad situarse en lo que matemáticos y físicos denominan el estado crítico. Estado crítico será aquel estado en el que el equilibrio entre el orden y el desorden permita la máxima fluidez de las relaciones sociales y, como consecuencia, el mayor grado de satisfacción de las personas que integran dicha sociedad; es decir, a aquel estado en el que la libertad de los individuos y la evolución social sea mayor.

3.2. Principio de legalidad

El *principio de legalidad*, contemplado en el artículo 14 de la Constitución Política de los Estados Unidos Mexicanos, señala que no se podrá imponer pena o medida de seguridad alguna si no es por la realización de una conducta que previamente ha sido descrita en la ley como delito, cuya sanción debe, igualmente, estar establecida en ley.[14]

[14]Aquí cabría hacer la anotación de que al mencionarse expresamente la palabra ley en la Constitución misma, debe entenderse a ésta como el producto del proceso legislativo, es decir, como ley en sentido material y formal. Al ser clara la

Este principio, que sintetiza la fórmula latina *nullum crimen, nulla poena sine lege*, exige no sólo que los órganos del Estado ajusten el ejercicio de su poder a lo establecido por la ley, sino también que la propia ley penal que se origina por tal ejercicio, esté diseñada con claridad y precisión, de suerte que de su contenido se derive seguridad jurídica para los gobernados.[15]

Puede afirmarse que, con ciertas salvedades de origen, este principio de algún modo se observa en la legislación federal penal sustantiva que cuenta con un catálogo de delitos y de penas, describiendo en lo esencial la materia de regulación de la norma penal y la amenaza penal correspondiente.

En México se generaron nuevas formas delictivas, por lo que se plantearon dos posibles soluciones; el incluir a los delitos informáticos dentro de los tipos penales existentes, o bien la creación de títulos y capítulos para éstos por su contenido tecnológico y gran cantidad de elementos normativos presentes; situación que dificulta la aplicación estricta del

---

Constitución y precisar el término ley, no cabe lugar a la interpretación, por lo que de este precepto se derivará la inconstitucionalidad de múltiples tipos penales que hacen referencia a reglamentos e, incluso, a normas oficiales mexicanas, normas jurídicas que no pueden integrar un delito pues en el texto constitucional no se emplea la palabra orden jurídico o norma jurídica, sino precisamente ley, que aunque coloquialmente puede entenderse en un sentido más amplio, jurídicamente sólo puede entenderse, en forma técnica, como la ley en sentido formal y material.

[15]Luigi Ferrrajoli (1995), argumenta que se ha producido una ampliación indeterminista del campo de lo designable como bienes tutelados, a través de la utilización de términos vagos, imprecisos o, lo que es peor, valorativos, que derogan la estricta legalidad de los tipos penales y brindan un amplio espacio a la discrecionalidad y a la «inventiva» judicial.

principio de legalidad que entraña la seguridad jurídica de los gobernados, ya que al estar integrado el tipo penal por múltiples elementos, algunos incluso ajenos a la propia legislación informática, origina una remisión normativa (problema propio de la normas penales en blanco). Aspecto que sin duda abrirá un capitulo nuevo para la jurisprudencia y la doctrina en torno al contenido de los preceptos legales penales informáticos y su alcance en su aplicación. Además porque en muchos casos no está determinado el modelo de delitos previstos entre los de mera conducta, resultado o de riesgo.

3.3. Principio de culpabilidad

El concepto de culpabilidad puede entenderse desde tres ángulos, el primero como categoría dogmática de la teoría del delito, el segundo como fundamento del principio desprendido del aforismo latín *nulla poena sine culpa* y el tercero como argumento legitimador de la pena y del *ius puniendi*.

Partiremos pues, de entender el concepto como principio del Derecho Penal, según el cual se hace corresponder la consecuencia penal a la existencia de ésta, *no hay pena sin culpabilidad*, por esta razón es instrumentalizada por el Derecho Penal, de tal suerte que un derecho penal de culpabilidad es contrario a un derecho penal de resultado y a un derecho penal de autor. En una interpretación del artículo 22 constitucional cuando determina: *Toda pena deberá ser*

proporcional al delito que sancione y al bien jurídico afectado, se obliga a establecer que en todos los tipos penales deben contemplar un bien jurídico tutelado para determinar la proporcionalidad de la pena con la afectación. Por ello es importante identificar el bien jurídico tutelado en los delitos informáticos en cada caso concreto.

El principio de culpabilidad se refiere entonces, a que la medida de la pena deberá corresponder al grado de culpabilidad del sujeto, esto es, el límite de la pena no deberá rebasar el límite de la culpabilidad. De tales ideas se desprende que la culpabilidad constituye tanto el fundamento como el límite de la pena relacionada con la lesión al bien jurídico tutelado.

4.-Marco Jurídico Internacional de la Cibercriminalidad

Ante el panorama de cibercriminalidad la comunidad internacional reaccionó con una serie de conferencias, convenciones, congresos y eventos internacionales, que derivaron en acuerdos, criterios, principios y medidas tendentes a dar solución a los problemas generados por las nuevas conductas delictivas, ya que por el carácter transnacional de estos delitos y la posibilidad de cometerlos desde cualquier parte del mundo, pueden afectar intereses de un Estado distinto de aquel en el que se realiza la acción, lo que provoca una serie de problemas como son los de la legislación y la jurisdic-

ción aplicable al caso y las necesidades de cooperación para extradición internacional. A continuación se mencionan las principales:

- 1981: El Consejo de Europa abre a la firma el Convenio número 108, para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, constituyéndose como el primer instrumento internacional que contiene un marco normativo respecto al tratamiento automatizado de los datos de carácter personal.
- 1985: La Organización de Cooperación y Desarrollo Económico (OCDE), publica una lista mínima de los delitos informáticos que los gobiernos signatarios podían incluir dentro de sus códigos penales, tales como; el fraude informático, el acceso ilícito a un sistema informático, la reproducción no autorizada de un programa de computadora, el sabotaje electrónico, el daño a los datos o a los programas informáticos, la interceptación no autorizada de datos, entre otros.
- 1990. El décimo tercer congreso internacional de la Academia de derecho comparado en Montreal Canadá y el Octavo Congreso Criminal de la ONU.
- 1992. Conferencia de Wuzburgo Alemania.
- 2000: En el marco del Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, celebrado cada cinco años

desde 1955, se propone la formulación de políticas gubernamentales encaminadas a la prevención y control de los delitos informáticos, así como la mejora de las capacidades en cuanto a enjuiciamiento de los mismos.

- 2001: El Consejo de Europa preocupado por el riesgo que implica la criminalidad cibernética, abre a la firma el Convenio sobre la ciberdelincuencia también conocido como Convenio de Budapest; instrumento internacional que reconoce la necesidad de cooperación internacional en materia penal, garantizando la tipificación como delito de los actos que ponen en peligro la confidencialidad, integridad y disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de los mismos.[16] En éste se establecen tres aspectos fundamentales. A) armonización de las normas penales sustantivas aplicables a las conductas delictivas que tienen como ámbito el entorno informático, B) Establecimiento de reglas procesales penales para facilitar la investigación de la criminalidad informática y C) la instrumentación de un sistema de cooperación internacional en el combate a estas conductas.

[16]Fue aprobado en la 109 reunión del Comité de Ministros del Consejo de Europa el 8 de noviembre de 2001, se abrió a firma en Budapest el 23 de noviembre del mismo año, y entró en vigor el 1 de julio de 2004, a partir del 28 de octubre 2010, 30 estados firmaron, ratificaron y se adhirieron a la Convención, mientras que otros 16 estados firmaron la convención, pero no la ratificaron.

- 2006. Protocolo Adicional a la convención sobre cibercrimen en materia de racismo y xenofobia.
- 2014. Convenio Iberoamericano de cooperación sobre investigación, aseguramiento y obtención de prueba en materia de ciberdelicuencia.
- Proyecto de Convenio de Stanford.[17]
- Ley modelo de Commonwealth sobre delitos informáticos y relacionados con la informática.[18]

De estos instrumentos internacionales podemos derivar una serie de conclusiones que en cierta medida definen los principios rectores de una política criminal informática que determina en cierto modo lo que ha pasado en nuestro país. No todos los documentos tienen carácter vinculante o pertenecen al denominado Soft Law, excepto aquellos que reúnen las características que exige nuestra legislación en materia de tratados internacionales aun cuando está pendiente la ratificación de la principal que es la Convención de Budapest, no obstante, las declaraciones o recomenda-

[17]Además, hay varias iniciativas científicas, como el proyecto de convenio internacional de Stanford (CISAC) elaborado como medida de seguimiento de la conferencia auspiciada por la Universidad de Stanford en los Estados Unidos en 1999 y el Cybercrime Legislation Toolkit de la UIT, preparado por la American Bar Association y otros expertos. No obstante, el impacto mundial de estos enfoques es limitado, en la medida en que sólo son aplicables a sus Estados miembros.

[18]La Ley Modelo de la Commonwealth sobre Delitos Informáticos contiene disposiciones relativas al derecho penal y procesal y la cooperación internacional; sin embargo, el impacto se limita a los países de la Commonwealth. www.cinu.mx/.../docs/delincuentes%20ciberneticos.pdf

ciones de congresos o eventos especializados en la materia han sido útiles para construir las directrices de la política criminal en materia de ciberdelitos y para derivar los principios orientadores en la materia.

5.- LOS BIENES JURÍDICOS PROTEGIDOS EN LA LEGISLACIÓN PENAL FEDERAL DE MÉXICO

En una cultura democrática de un estado de derecho penal mínimo y garantista, el bien jurídico se entiende como todo interés, valor o derecho que merece la protección del orden jurídico;[19] específicamente, por bien jurídico penal, como lo denomina Mir Puig, se entenderán aquellos intereses, valores, o derechos que merecen y tienen la protección de las normas de carácter penal. Estos intereses, valores o derechos resultan relevantes para mantener la armonía y el equilibrio de la vida social, su protección se relaciona con la seguridad, el bienestar y la dignidad humana en una formación social.

Estos bienes jurídicos están consagrados en la Constitución y son reconocidos en el Derecho Internacional, porque de ser lesionados o puestos en riesgo, se justifica la intervención del poder punitivo en ultima instancia, aquí surge el concepto de bien jurídico penalmente tutelado o

[19]Ignacio Berdugo de la Torre (1992) sostiene que el catálogo de bienes jurídicos tutelados por un determinado ordenamiento es el exponente de los intereses para el mantenimiento y evolución de un concreto modelo social.

protegido. En consecuencia, y aun cuando el principio de bien jurídico protegido penalmente, haya sido construido para limitar el ejercicio del poder punitivo, es indiscutible que en el actual panorama de la sociedad de la información y de la sociedad del riesgo, hay un serie de comportamientos que justifican la intervención penal para la protección de esos intereses en juego, no obstante, se corre el riesgo de que en aras de su excesiva protección se genere la expansión irracional del derecho penal.

Para Bustos (1997) los bienes jurídicos, considerados materialmente son:

> relaciones sociales concretas que surgen como síntesis normativa de los procesos interactivos de discusión y confrontación que tienen lugar dentro de una sociedad democrática. Son dinámicos pues están en permanente discusión y revisión. Por ello se explica ahora, la emergencia de los intereses, valores o derechos producto de la gran transformación digital, que ha provocado la aparición de las tecnologías de la informática y la comunicación y las nuevas relaciones que se dan entre diversos actores sociales.

Rolan Hefenndehl refiere los diversos criterios teóricos sobre el tema, y señala que los bienes jurídicos suponen aquellos presupuestos valiosos y necesarios para la existencia; otros los definen como aquellas circunstancias dadas o finalidades que son útiles para el individuo y su libre desarrollo en el marco de un sistema social global estructurado sobre la base de la concepción de estos fines o para el funcionamiento del propio sistema;

algunos más los han descrito como presupuestos instrumentales necesarios para el funcionamiento del sistema social y su supervivencia.

Desde esta perspectiva habrá que ubicar el tema sobre la importancia que tiene hoy en día la funcionalidad[20] de la adecuada gestión de la información y la relevancia de su protección y seguridad social e individual. Conviene entonces, recordar la clasificación teórica de los bienes jurídicos, en individuales y en colectivos o supraindividuales. Los primeros son fáciles de identificar y de proteger penalmente, pues se trata de intereses, valores o derechos que son ejercidos por una persona en lo individual y que afectan sólo a ésta, mientras que en el caso de los segundos, se asevera que tienen un carácter difuso, ante la imposibilidad de identificación del titular de los mismos y, en consecuencia, ofrecen cierta dificultad en su protección. No obstante por seguridad jurídica habrá que entender estos intereses macrosociales siempre vinculados a un interés humano concreto, como lo señala Hernán Hormazábal Mallareé (1997).

---

[20]José Urquizo (1998): El tema de los bienes difusos, o bienes colectivos que por su contenido y alcance expresan la funcionalización del sistema, del orden económico, la salud pública, el medio ambiente, recogen nuevos intereses y el proceso de asimilación viene presidido por una fuerte tensión en el Derecho penal. Tal como lo muestra el profesor Portilla Contreras, resulta discutible si en rigor son bienes jurídicos o sólo funciones y utilizando el análisis de Hassemer deja planteado que estos intereses no son ya bienes jurídicos en el sentido tradicional, sino objetivos de organizaciones políticas, sociales o económicas, por lo que el Derecho Penal no tutela ya víctimas sino funciones. El riesgo de la asunción de esquema de tutela de funciones radica en transformar el injusto penal en un ilícito de mera transgresión que, en realidad, no cambia, tampoco si el concepto de función se sustituye por el substancialmente equivalente de bien social, propuesto por acreditada doctrina. ttp://sisbib.unmual/publicacione que

De ahí que se proponga considerar de *interés colectivo* la adecuada circulación de la información en el marco de esta sociedad red, en la medida que esta sociedad global se encuentra determinada por el correcto funcionamiento del intercambio de información para la realización de una serie de actividades humanas, por ejemplo la información que se utiliza para el tráfico aéreo, que en la actualidad se cuenta por infinidad de vuelos internacionales al día (Soto, 2003).

En cuanto al bien jurídico que se pretende tutelar en los delitos informáticos, surge una discusión en torno a dos posiciones doctrinales. Por un lado encontramos un sector que niega la existencia de nuevos bienes jurídicos dentro de los delitos informáticos; en este sentido Bramant Arias Torres afirma que "en realidad no existe un bien jurídico protegido en el delito informático, porque en realidad no existe como tal el delito informático. Esto no es más que una nueva forma de ejecución de conductas que afectan bienes jurídicos que ya gozan de protección por el derecho penal".

Lo anterior, sería aplicable a los denominados delitos computacionales que se identifican así, porque el medio de comisión son las tecnologías de la información o la comunicación y el valor protegido es distinto al valor económico de la información. Esta posición es fuertemente criticada pues confunde a los delitos informáticos con los denominados delitos computacionales, ya que los delitos computacionales son aquellas conductas ilícitas que realizadas por medio de un sistema o una red informática o con cualquier otro

medio informático, lesionan bienes jurídicos ya existentes y los delitos informáticos son nuevos comportamientos ilícitos que afectan nuevos intereses.

Por otro lado, un gran sector de la doctrina a nivel internacional coincide en que el desarrollo de los medios informáticos ha traído consigo nuevos intereses sociales, que necesitan la protección del derecho penal. Téllez Valdés (2006) afirma que debido al gran valor económico que ha adquirido la información en los últimos años, se ha convertido en un nuevo bien jurídico que merece protección penal.

Al respecto, Luis Miguel Reyna Alfaro (citado en Castro, 2002) menciona:

> Los constantes avances tecnológicos en materia informática han propiciado la aparición de nuevos conceptos, generando así mismo la modificación de otros tantos, enriqueciéndolos la mayoría de ocasiones, así el contenido del término información, que según la definición de la Real Academia de la Lengua Española significa: 'enterar, dar noticia de algo' y que en términos legos hubiera significado tan sólo una simple acumulación de datos, se ha ampliado, transformándose como advierte Gutiérrez Francés: 'en un valor, un interés social valioso, con frecuencia cualitativamente distinto, dotado de autonomía y objeto del tráfico'. Hoy en día no resulta suficiente poseer la información, es necesario además tener la capacidad de almacenarla, tratarla y transmitirla eficientemente, de allí que 'la información' deba ser entendida como un proceso en el cual se englobe los tres supuestos (almacenamiento, tratamiento y transmisión). (...) Así podemos decir que el interés social digno de tutela penal

> sería: la información (almacenada, tratada y transmitida a través de sistemas informáticos),...

En relación con lo anterior, la doctrina se encamina a reconocer que la información es un bien jurídico de carácter supraindividual o colectivo, además se advierte que la naturaleza particular de los delitos informáticos, la ubican en las clasificaciones teóricas dentro de los delitos pluriofensivos, pues simultáneamente al ataque al derecho a la información, se pueden dañar intereses individuales o públicos tales como la intimidad, la propiedad, la propiedad intelectual, la seguridad pública, la seguridad nacional e internacional, la confianza en el correcto funcionamiento de los sistemas informáticos o seguridad informática, entre otros (Contreras, 2003).

> En definitiva y tal como lo adelantáramos, atendiendo a las características de esta nueva era y sus implicancias ya descritas, entendemos que el bien jurídico en los delitos informáticos es la información en sí misma, en todos sus aspectos, como interés macro-social o colectivo, porque su ataque supone una agresión a todo el complejo entramado de relaciones socio-económico-culturales, esto es, a las actividades que se producen en el curso de la interacción humana en todos sus ámbitos y que dependen de los sistemas informáticos. Disentimos, acorde con la postura sustentada en torno al bien jurídico tutelado en los delitos informáticos, con las tradicionales distinciones doctrinales de estas conductas ilícitas en delitos informáticos de carácter económico y aquellos que atentan contra la privacidad. Reyna (citado en Castro, 2002).

De acuerdo con el análisis de la legislación federal mexicana y la estatal de Chiapas, en el ámbito de los delitos informáticos, el bien penalmente tutelado es la seguridad de la información; así se tendrá como regla general, que el bien jurídico genérico protegido es el valor intrínseco de la información y, de manera particular, el bien se identifica a partir de cada delito. En este trabajo abordaremos los correspondientes a seguridad informática y protección de los datos personales o protección de la privacidad o intimidad de las personas.

En muchos casos, el bien penalmente tutelado no se encuentra expresamente referido en el texto de la ley; en México, el Código Penal comúnmente lo indica o proporciona datos implícitos respecto de los valores que pretende proteger. En el caso de los delitos informáticos, el bien penalmente tutelado genérico, es la información, sin embargo el legislador al modificar el título nueve del ordenamiento, agregó la descripción de la conducta sin referirse al bien jurídico tutelado, mismo que hay que desprender de su interpretación teleológica y sistemática. Por esta razón es que hay que distinguir el bien tutelado común a todos los delitos previstos en el Título de los denominados "delitos informáticos" y el bien específico tutelado, que será el que se señale en cada caso.

En este tenor, tenemos que en la interpretación o aplicación a un caso concreto:

> el intérprete tiene que partir del (hecho) típico, como expresión de un especifico conflicto intersubjetivo de intereses que constituye un requisito estructural del tipo delictivo y que justifica su castigo mediante una sanción penal. Y para individuar esta relación conflictiva intersubjetiva en el ámbito específico de los delitos informáticos, el intérprete tiene que ir necesariamente más allá del lenguaje técnico informático empleado por el legislador en la formulación de los tipos. (Pérez y Díaz, 2014)

Desde la perspectiva dogmática, en el caso de los delitos previstos en la Ley Federal de Protección de Datos, el derecho humano a la privacidad o a la intimidad es el derecho que tiene cada persona de disponer de una esfera, espacio privativo o reducto inderogable de libertad individual y que no puede ser invadido por terceros. Un concepto amplio, podría entenderlo como el control y/o la libertad de elegir cómo, cuándo y por quién cierta información (ya sea mental, física o electrónica) podrá ser revelada a otros. Este interés o valor concedido socialmente a los particulares respecto a su información sensible, no es el directamente protegido, al menos en el caso del capítulo segundo que analizaremos, sino que es objeto de protección en la Ley de Protección de Datos de Particulares, ordenamiento vinculado al Código Penal en el caso de resolver algunos de sus elementos normativos relativos al bien jurídico de la seguridad informática.

6.- MARCO JURÍDICO Y DOCTRINAL DE LOS DELITOS INFORMÁTICOS

En el desarrollo de la disciplina jurídica que surge de la relación del derecho y las tecnologías de la información y las comunicaciones, José Palomino Martin (2006) afirma que:

> hemos constatado la existencia de un incipiente relación entre la ciencia penal y la ciencia de la información y la comunicación, cada vez, más intensa, fecunda e inevitable, fruto de la nueva sociedad de la información, en cuyo marco de colaboración interdisciplinar viene aflorando un área del conocimiento que hemos denominado informática jurídico penal, que abarca los estudios sobre derecho penal informático, es decir el relacionado con las nuevas tecnologías, y los avances que se suceden en la informatización o informático del derecho penal.

Estudiar al derecho penal informático[21] desde la perspectiva dogmática, implica hacer un análisis de la normatividad existente y describir el estado de la cuestión para fines de operación jurídica, cabe mencionar que no significa alinearse a la expansión penal en México o creer que el derecho penal es el principal instrumento para solucionar este

[21]Díaz (2010) comenta:

> Todos los elementos conflictivos anteriormente enunciados están claramente interrelacionados, de manera que se influyen mutuamente, y cualquier solución pasa por una visión conjunta de todos ellos. Son pues las peculiaridades que plantean los nuevos delitos las que justifican su análisis particular; luego es necesario agrupar los tipos con rasgos y problemas comunes para un tratamiento adecuado y armonioso. A estos tipos comunes se les vendrá a llamar ciberdelitos, y a la parte del Derecho Penal que los estudia, Derecho Penal Informático.

tipo de problemas; sin embargo, en la actualidad las normas penales informáticas vigentes, aún están sujetas a prueba de eficacia, para corroborar si en alguna medida responden a la solución de los problemas de seguridad informática fundamentales.

Desde luego considero que deben establecerse distintos niveles de tratamiento penal en función de la calidad de los sujetos activos del delito, es decir distinguir en la legislación penal informática entre sujetos convencionales y delincuencia poderosa, organizada, característica de la economía global; este trato diferenciado provocará consecuencias en el modelo de imputación, en la garantías procesales que deben observarse y el tipo de penas adecuadas según los sujetos del delito, no será remota la posibilidad de que en su momento se encuentre la solución en una legislación especial para este ámbito.

Lo anterior origina que varios países se adhieran a las recomendaciones internacionales mediante la promulgación de una serie de instrumentos normativos locales.[22] El orden penal federal mexicano no contemplaba a los delitos informáticos[23] sino hasta el 17 mayo del año 1999, cuando se publicó

[22]Reacción que sintetiza al denominado Principio de conjunción, que determina la unión en un mismo orden jurídico de la norma internacional y la nacional, debido a que la primera en cada vez más nacional, más local, es decir de aplicación inmediata; lo que distingue a los órdenes jurídicos internos por el grado en que incorporan el derecho internacional al propio.

[23]En el ámbito de las entidades federativas el Código Penal del estado de Sinaloa, tenía algunos delitos informáticos legislados desde 1996.

la reforma al Título noveno del Código Penal Federal denominado "Revelación de secretos y acceso ilícito a sistemas y equipos de informática", que adicionó un segundo capítulo, incluyendo la aparición de siete nuevos tipos penales.

Cabe mencionar que en lo que se refiere a persecución, la Policía Federal dependiente de la Comisión Nacional de Seguridad, cuenta con una policía cibernética que se encarga de identificar y desarticular organizaciones dedicadas al robo, lenocinio, pedofilia, tráfico y corrupción de menores, elaboración, distribución y promoción de pornografía infantil, etc., por cualquier medio informático; así mismo realiza patrullaje anti-hacker, utilizando la Red como un instrumento para detectar a delincuentes que organizan sus actividades delictivas en la red.

Como podemos notar, en nuestro país, el derecho penal informático aun se encuentra en su etapa primaria, si bien el Código Penal Federal vigente y las legislaciones penales de diversas entidades federativas contemplan tipos penales informáticos, éstos delimitan de alguna forma las conductas de los sujetos activos, razón por la que sería conveniente llevar a cabo una reforma penal integral que garantice la seguridad jurídica de los gobernados.

No obstante, como ya se ha dicho, el derecho penal no debe convertirse en el principal medio de solución de los problemas informáticos, sino que deberá emplearse cuando todos los otros hayan fallado en su cometido; en este sentido cabe considerar el hecho de ampliar las capacidades y

facultades de la policía cibernética, con el fin de realizar una labor de prevención más amplia y efectiva.

7.- CONCEPTO DE DELITO INFORMÁTICO

Previo el análisis sistemático de los delitos informáticos, revisaremos una serie de definiciones del delito informático en estricto y amplio sentido, para indicar desde qué perspectiva y qué elementos haremos nuestro estudio. Aclaro que estas definiciones han sido elaboradas por expertos en Derecho Informáticos, Criminólogos y Penalistas, que al estar supeditas al lenguaje utilizado por las diversas legislaciones nacionales, tendrán un contenido distinto en cada país, y la doctrina nacional también las definirá de manera diferente.

En 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) acuñó el término *computer crime* determinándolo como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el proceso automático de datos y las transmisiones automáticas de datos."

El concepto proporcionado desde 1986 por la criminóloga María de la Luz Lima nos dice, que:

> el delito electrónico en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, es cualquier acto ilícito

> penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin.

Esta definición no se refiere al concepto de delito informático y tiene la característica de ser una definición que se decanta sobre el tema electrónico, pero tiene la virtud de ser una concepción amplia al indicar que la computadora sea un método, medio o fin.

El experto en derecho informático Julio Téllez Valdés entiende al delito informático a partir de su forma típica o atípica, determinando a la primera como "la conducta típica, antijurídica y culpable en que se tiene a las computadoras como instrumento o fin" y a la segunda como "aquellas actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".

El experto Español Davara Rodríguez (2002) define al Delito informático como, "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software." Esta definición concede el sitio al tema penal remitiendo a la teoría del delito y precisa un campo informático con el lenguaje propio de la materia.

Los profesores chilenos Marcelo Huerta y Claudio Líbano (citados en Acurio) definen los delitos informáticos como:

> todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro.

Denominación amplia que no distingue entre informáticos y computacionales, según se usen los sistemas informáticos o la computadora, como medio o fin.

Sergio G. Torres define a los delitos informáticos como:

> acciones típicas, antijurídicas y culpables, que recaen sobre la información, atentando contra su integridad, confidencialidad o disponibilidad, como bien jurídico de naturaleza colectiva o macro-social (abarcativo de otros intereses, vgr.: propiedad común, intimidad, propiedad intelectual, seguridad pública, confianza en el correcto funcionamiento de los sistemas informáticos, fe pública, etc.), en cualquiera de las fases que tienen vinculación con su flujo o intercambio (ingreso, almacenamiento, proceso, transmisión y/o egreso), contenida en sistemas informáticos de cualquier índole, sobre los que operan las maniobras dolosas.

Han sido muchas las denominaciones que se han utilizado para designar a las conductas ilícitas en las que se tiene a la computadora como instrumento para llevarlas a

cabo: delitos informáticos, delitos electrónicos, delitos relacionados con la computadora, crímenes por computadora, delincuencia relacionada con el ordenador; sin embargo no existe una definición de carácter universal, por lo que será de vital importancia encontrarla a partir de la cooperación internacional.

Un documento importante en el plano internacional que le da seguimiento a la Convención Europea, lo define como "aquellas conductas ilícitas que afectan el bien jurídico información en formato digital, entendido dichas afectaciones a la confidencialidad, integridad, disponibilidad o uso de la información o de sus sistemas informacionales de soporte." (Iriarte, 2007)

Por nuestra parte definimos al delito informático, en estricto sentido en México, y partiendo del contenido de la legislación federal, como la conducta típica antijurídica y culpable que afecta la seguridad informática y el derecho humano de la intimidad de las personas, mediante el tratamiento doloso de los datos, que se distinguen de los demás supuestos de los llamados delitos computacionales o electrónicos[24] donde los equipos o sistemas informáticos constituyen medios para la consumación de otras conductas que afectan bienes jurídicos distintos a la seguridad informática.

[24]Son aquellas conductas ilícitas que empleando TIC, afectan bienes jurídicos previamente reconocidos en la legislación penal vigente, distintos al de la información en formato digital, siempre que el tipo penal lo permita.

8.- MÉTODO PARA EL ANÁLISIS DOGMÁTICO DE LOS DELITOS INFORMATICOS EN MÉXICO

A continuación presentamos el esquema que se adopta en este artículo para el análisis de cada uno de los delitos.

1) Elementos subjetivos

a. Dolo/culpa.- Existirán supuestos en los cuales la conformación del tipo requiera expresamente que una cierta conducta se realice dolosamente, otros en que se permita su comisión culposa, pero cuando no se establezca ninguna referencia al dolo o a la culpa, habrá que consultar el artículo 60 del Código Penal Federal a fin de determinar si, en el caso concreto, esa conducta acepta o no la comisión culposa. A partir de las reformas penales de 1994, no cualquier conducta admite comisión culposa, sino sólo aquéllas contenidas en dicho artículo. Fuera de los casos que contempla el catálogo de este precepto, o de aquellos en que expresamente se señala que se pueden cometer culposamente ciertas conductas, sólo se podrán cometer los delitos en forma dolosa; es decir, no habrá delito cuando no se pueda acreditar el dolo. Las directrices internacionales de los distintos documentos elaborados con respecto a los delitos in-

formáticos recomiendan solo incluir los supuestos dolosos y no considerar los culposos o imprudenciales. En específico en el Convenio de Budapest, en los artículos segundo, cuarto y quinto de dicho instrumento que se refiere a los comportamiento dolosos y sin autorización de acceso ilícito y a los atentados en contra de la integridad de los sistemas y de los datos.

2) Elementos objetivos

a. Sujeto activo/determinada calidad del sujeto activo.- Se refiere a quien comete el delito y a las características que la ley exija de este sujeto en el caso concreto (sexo, la calidad de servidor público, la calidad de dueño, etc.). Cuando la ley no prevea nada específico sobre el sujeto activo, se entenderá que el delito puede ser cometido por cualquier persona. En todos los delitos habrá siempre un sujeto activo, aunque no en todos los casos se requiera una determinada calidad de éste. En el caso de los delitos contra la seguridad informática que analizamos, el legislador hace una alusión al sujeto activo, cuando dice el que no esté autorizado, así que serán excluidos de esta conducta las personas que si estén autorizadas para acceder a la información contenida en los equipos o sistemas.

b. Sujeto pasivo/determinada calidad del sujeto pasivo.- Las reflexiones hechas en el inciso a), son aplicables al sujeto pasivo del delito, es decir, el titular del bien penalmente lesionado o puesto en peligro. Al igual que en el punto anterior, puede decirse que siempre habrá un sujeto pasivo en los delitos, aunque no siempre sea necesaria alguna determinada calidad del mismo para la integración del tipo. En los primeros supuestos estos delitos contra seguridad informática, no determina sujeto pasivo, por lo que se entiende que podrá ser ofendido cualquier persona que tenga derecho sobre la información contenido en equipos y sistemas de computo que sean vulnerados, en posteriores supuestos se refiere al Estado a dependencias públicas (caso de Chiapas), a instituciones de Seguridad Pública y las instituciones del Sistema Financiero.
c. Conducta/verbo(s) rector(es). - Existen uno o varios verbos en la descripción de un delito -llamado verbo o verbos rectores- que sirven para identificar las conductas que se sancionarán penalmente. La conducta es más completa que el verbo; por ejemplo, en el abuso de confianza se habla de la transmisión, como verbo rector, aunque la conducta será la transmisión de la tenencia y no del dominio. El verbo rector se identifica como aque-

lla forma en que se manifiesta la conducta delictiva; no siempre se presenta conjugado en infinitivo (con terminaciones ar, er o ir), sino que puede también estar referido a un sujeto (quien transmita la tenencia...). La conducta o conductas y el verbo o verbos rectores, son un elemento común a todos los delitos. En el presente caso los verbos previstos, son destruir, modificar, copiar conocer, tratar información, entre otros verbos rectores. Esta figura incorpora el denominado comportamiento identificado como Cracking[25] que consiste en el "Acceso ilícito a sistemas y equipos de informática"

d. Especiales medios de comisión.- Existen ocasiones en las cuales se exige que la acción se ejecute de alguna determinada forma, y si no se constata este medio de comisión, no existirá delito. Cuando no se establece ningún medio especial de comisión, basta con realizar la conducta prevista por el tipo penal, ejecutando únicamente el verbo rector precisado; consecuentemente, se puede afirmar que

[25]En informática, conducta delictiva en donde un individuo denominado cracker altera, modifica, elimina, borra los datos de un programa informático o de un documento con la finalidad de obtener un beneficio de dicha alteración; puede referirse a varias prácticas similares, o al conjunto de ellas: Password cracking: quebrar la seguridad de una contraseña o password. System cracking: quebrar la seguridad de un sistema informático.Software cracking: quebrar la seguridad anticopia o antipiratería de un software.

no todos los delitos exigen una especial forma de comisión, o un especial medio para ejecutarse. En este caso no se prevé violencia o algún medio de comisión especifico, porque de haber redactado el legislador por ejemplo, "el que violando algún mecanismo de seguridad física o lógico accede, conozca, copie, destruya, información contenida en equipos o sistemas de computo, podríamos tomar que sería un medio de comisión, pero no es el caso actual".

e. Resultado.- Dentro de la clasificación que hace la doctrina penal, existen los delitos de resultado, delitos de peligro y de mera conducta o desobediencia. En los primeros, sí es necesario que se modifique el mundo exterior y que se provoque un daño real. En cambio, existen delitos en los que la conducta no provoca un resultado dañino, sino que es considerada peligrosa en sí misma y el legislador exige un riesgo concreto o lo plantea abstracto, independientemente de que ocasione o no un resultado. En el caso de los delitos informáticos, hay supuestos de daño informático y en otros delitos de mera conducta que implican el conocimiento de la información sin que haya menoscabo de ella, sólo que ataca uno de los elementos de la seguridad informática, que es precisamente el carácter

confidencial de ella[26]. No advertimos ningún supuesto de delitos de peligro ni en el Código Penal ni mucho menos en la Ley Federal de Protección de Datos en posesión de particulares, tampoco en la legislación Penal de Chiapas.

f. Objeto.- Se refiere a aquello sobre lo que recae la conducta. Por ejemplo, en el caso del robo, el objeto es un bien ajeno mueble, pues no se puede efectuar robo sobre otro tipo de bienes. Este es un elemento siempre presente en los delitos, ya que el verbo rector debe estar referido a alguna situación concreta; gramaticalmente, la conducta se debe aplicar a "algo". Este puede ser un objeto material o un objeto jurídico. En el caso que nos ocupa las acciones prohibidas recaen en la información contenida en equipos o sistemas de cómputo. El objeto material son los datos electrónicos contenidos en la parte física de la computadora.

g. Bien penalmente tutelado. En muchos casos, el bien penalmente tutelado no se encuentra expresamente referido en el texto de la ley. Como ya vi-

[26]María Acale Sánchez (2002): Esta acepción del resultado es pues la que sostiene la diferenciación entre los delitos de mera actividad y los de resultado; en este sentido, hoy se entiende que los delitos de mera actividad son aquellos en los que dentro del tipo delictivo en concreto, el legislador ha incluido un comportamiento pero no ha prestado atención, esto es, no ha incorporado como elemento típico, el efecto natural provocado y separable del mismo. e-spacio.uned.es/fez/eserv/bibliuned...2002-10-5010/Documento.pd

mos anteriormente, el bien penalmente tutelado es aquel valor que se encuentra detrás de la norma, que motivó que una conducta se considerara nociva socialmente y se sancionara penalmente por tal gravedad. Comúnmente, la estructura del Código Penal indica en sus Títulos y en sus Capítulos el bien penalmente tutelado, o da una idea muy cercana respecto de los valores se pretende proteger. En el caso de los delitos contra la seguridad informática el bien jurídico es precisamente la integridad, disponibilidad y confidencialidad de la información, aspectos que garantizan la seguridad informática[27]. Esto para distinguir de otros delitos que tienen relación con la protección jurídica de la información sensible, por ejemplo los que protegen los datos personales o del derecho de la intimidad, o de la información económica y cuantificable, o los de la seguridad interior del estado.

h. Circunstancias de tiempo, modo, lugar u ocasión.- Existen casos en los cuales el tipo penal prevé la realización de alguna circunstancia para la constitución del tipo penal, aunque lo más común es que estas circunstancias sólo sirvan para efectos

[27]En el Convenio de Budapest, la parte inicial de las infracciones penales se encuentra organizado con este criterio. "Capítulo II – Medidas que deben ser adoptadas a nivel nacional Sección 1 – Derecho penal material Título 1 – Infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos"

de calificar a un tipo base. Por ejemplo, se establece el tipo básico del robo, indicando que consiste en el apoderamiento de un bien ajeno mueble sin consentimiento y sin derecho de la persona que puede disponer de éste conforme a la ley. Esta es una descripción muy amplia, y que prevé una cierta penalidad. Sin embargo, después se contemplan otras hipótesis, como realizarse en lugar cerrado (circunstancia de lugar) y en cuyo caso se aumentará la pena del tipo base; igualmente, también se sancionará con mayor severidad al robo efectuado con violencia (modo), o cuando se cometa aprovechando las condiciones de confusión que se producen por una catástrofe (ocasión). Un ejemplo de circunstancias de tiempo, sería el hecho de que por ejemplo se requiriera, para integrar los elementos del tipo, que el delito sea cometido "de noche" o "después de horas de trabajo". En los delitos contra la seguridad informática previstos en el capitulo segundo del título noveno del Código Penal Federal de nuestro país (de manera semejante los de Chiapas), se refiere a que la realización de la conducta prohibida en equipos protegidos por algún *mecanismo de seguridad*, lo que se puede interpretar como un circunstancia de modo de acceso, porque al mencionar este aspecto relativo la seguridad informática, como son las claves o contrase-

ñas para el acceso, plantea una forma de violación a la seguridad informática. Pero también desde una interpretación literal, podría considerarse desde la perspectiva de la seguridad informática física, que cuando dice protegido por algún mecanismo de seguridad, incluye a estos, como sería el caso de alguien que entre violando una cerradura de una sala de computo, en donde los equipos no estén protegidos con alguna clave de ingreso, y realice las conductas prohibidas y se estará configurando el supuesto, dado que el legislador no hizo la referencia a que clase de mecanismo de seguridad se refería. Hace alusión que los sistemas o equipos estén protegidos por algún mecanismo de seguridad, y la interrogante es como llenar este contenido del término mecanismo, si incluye a los de la seguridad física, como las claves electrónicas para abrir una puerta de una sala de computo que son externos a los sistemas o equipos que sean objeto de vulneración con las conductas, o solamente se refiere a los mecanismos de seguridad del sistema y los equipos de cómputo, entonces hablaremos de mecanismos de seguridad lógica.[28]

[28]Es decir que la Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica. Los objetivos que se plantean serán:

i. Elementos normativos. Los elementos de esta categoría son abundantes en los tipos informáticos. Para determinarlos habrá que consultar la legislación que en materia informática se ha expedido hasta la actualidad, vale citar las Leyes Federal y General de Transparencia y acceso a la información pública, la Ley Federal de Protección de Datos personales en posesión de los Particulares y la Ley de la Sociedad de la Información Crediticia, Ley de Firma Electrónica Avanzada, así como todos los reglamentos que se desprenden de esta legislación ordinaria. Algunos de estos términos están definidos en el ámbito internacional, en particular en Convenio de Cibercriminalidad, o Convenio de Budapest, que en el caso de nuestro país se encuentra en proceso de ratificación y aun cuando hay un proceso de adopción de sus recomendaciones en el diseño que los legisladores federales y estatales han realizado, para los propósitos de su aplicación aun no es norma vigente.

---

1. Restringir el acceso a los programas y archivos. 2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan. 3. Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto. 4. Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro. 5. Que la información recibida sea la misma que ha sido transmitida. 6. Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos. 7. Que se disponga de pasos alternativos de emergencia para la transmisión de información. http://www.segu-info.com.ar/logica/seguridadlogica.htm

No obstante, para los efectos de compresión de los elementos normativos del tipo, es conveniente tener en cuenta esas definiciones.

- *Sistema informático*, designa todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos;
- *Datos informáticos*, designa toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función.

9.- ANÁLISIS DOGMÁTICO DE LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL FEDERAL

Titulo Noveno

Revelación de secretos y acceso ilícito a sistemas y equipos de informática

Capitulo II

Acceso ilícito a sistemas y equipos de informática[29]

[29]De manera semejante al Legislador Español, con este capítulo se incluye sanciones para castigar conducta de Hacking y Cracking, en el año de 2010, relacionado con el acceso no autorizado a datos y programas informáticos. En el articulo 615- ter del Código Penal Italiano, también se configuran tipos semejantes en sus estructura y

Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque perdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Primer párrafo

Conducta	Modificar, destruir o provocar pérdida de información
Bien Jurídico	La seguridad de la información
Realización dolosa/ culposa	Sólo admite la realización dolosa por el criterio de numerus clausus
Sujeto Activo	Cualquier persona que no esté autorizada.
Sujeto pasivo	Puede ser cualquier persona, no se establece calidad específica.
Objeto Material	Información contenida en Sistemas o equipos de informática

exigencias típicas. Violando las medidas de seguridad sin que el legislador las defina lo que se entiende que pueden ser la de seguridad lógica o las de seguridad física.

Circunstancias de tiempo, modo y lugar	Protegido por algún mecanismo de seguridad.
Especiales medios de Comisión	No exige
Elementos subjetivos específicos.	En el tipo penal básico: No se establecen.
Nexo causal	Delito de resultado que se traduce en la transformación o eliminación esencial de la información.
Elementos normativos	Sistemas de informática. Equipos de informática. Mecanismo de seguridad.
Sanción	Se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. De acuerdo con el artículo 211 bis 7, las penas previstas en este capítulo se aumentaran hasta en una mitad cuando se utilice la información en provecho propio o ajeno.

Segundo párrafo

Conducta	Conocer o copiar información
Bien Jurídico	La seguridad informática.
Realización dolosa/ culposa	Sólo admite la realización dolosa por el criterio de numerus clausus
Sujeto Activo	Puede ser cualquier persona que no esté autorizada.
Sujeto pasivo	Puede ser cualquier persona, no se establece calidad específica.

Objeto Material	Información contenida en sistemas o equipos de informática
Circunstancias de tiempo, modo y lugar	Protegido por un mecanismo de seguridad
Especiales medios de comisión	No exige
Elementos Subjetivos Específicos	No se establecen
Nexo causal	Delito de conducta que vulnera la confidencialidad de la información.
Elementos normativos	Sistemas de informática. Equipos de informática. Mecanismo de seguridad.
Sanción	Se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa. De acuerdo con el artículo 211 bis 7, las penas previstas en este capítulo se aumentaran hasta en una mitad cuando se utilice la información en provecho propio o ajeno.

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impon-

drán de seis meses a dos años de prisión y de cien a trescientos días multa.

A quien sin autorización conozca, obtenga, copie o utilice información contenida en cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública, protegido por algún medio de seguridad, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Primer párrafo

Conducta	Modificar, destruir o provocar perdida de información del Estado.
Bien Jurídico	La seguridad informática del Estado.
Realización dolosa/ culposa	Sólo admite la realización dolosa por el criterio de numerus clausus
Sujeto Activo	Puede ser cualquier persona que no esté autorizada.
Sujeto pasivo	El sujeto pasivo es el Estado.
Objeto Material	Sistemas o equipos de informática del Estado

Circunstancias de tiempo, modo y lugar	Protegido por un mecanismo de seguridad.
Especiales medios de comisión	No exige.
Elementos subjetivos Específicos	En el tipo penal básico: No se establecen. En el tipo penal calificado: se utilice la información en provecho propio o ajeno.
Nexo causal	Delito de resultado que se traduce en la modificación, destrucción o pérdida de información del Estado.
Elementos normativos	Sistemas de informática del Estado. Equipos de informática del Estado. Mecanismo de seguridad del Estado.
Sanción	Se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. De acuerdo con el artículo 211 bis 7, las penas previstas en este capítulo se aumentaran hasta en una mitad cuando se utilice la información en provecho propio o ajeno.

Segundo párrafo

Conducta	Conozca o copie información
Bien Jurídico	La seguridad informática del Estado
Realización dolosa/ culposa	Sólo admite la realización dolosa por el criterio de numerus clausus
Sujeto Activo	Puede ser cualquier persona no autorizada.
Sujeto pasivo	Puede ser cualquier persona, no se establece calidad específica.

Objeto Material	Sistemas o equipos de informática del Estado
Circunstancias de tiempo, modo y lugar	Protegida por un mecanismo de seguridad.
Especiales medios de comisión	Al que sin autorización.
Elementos subjetivos Específicos	En el tipo penal básico: No se establecen. En el tipo penal calificado: se utilice la información en provecho propio o ajeno.
Nexo causal	Delito de resultado que se traduce en el conocimiento o copia de información del Estado
Elementos normativos	Sistemas de informática del Estado. Equipos de informática del Estado. Mecanismo de seguridad del Estado.
Sanción	Se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. De acuerdo con el artículo 211 bis 7, las penas previstas en este capítulo se aumentaran hasta en una mitad cuando se utilice la información en provecho propio o ajeno.

Tercer párrafo

Conducta	Conozca, obtenga, copie o utilice información
Bien Jurídico	La seguridad informática de la seguridad pública.
Realización dolosa/ culposa	Sólo admite la realización dolosa por el criterio de numerus clausus
Sujeto Activo	Puede ser cualquier persona, no autorizada. Para el tipo calificado ser o haber sido servidor público en una institución de seguridad pública.

Sujeto pasivo	Puede ser cualquier persona privada o pública que tenga información de la seguridad pública.
Objeto Material	Cualquier sistema, equipo o medio de almacenamiento informáticos de seguridad pública
Circunstancias de tiempo, modo y lugar	Protegidas por algún medio de seguridad
Especiales medios de comisión	No exige.
Elementos subjetivos Específicos	En el tipo penal básico: No se establecen.En el tipo penal calificado: se utilice la información en provecho propio o ajeno.
Nexo causal	Delito de conducta que vulnera la seguridad de la información. De seguridad pública.
Elementos normativos	Seguridad pública. Sistemas de informática de seguridad pública. Equipos de informática de seguridad pública. Medio de almacenamiento de seguridad pública
Sanción	Se le impondrán de cuatro a diez años meses a dos años de prisión y de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, destitución e inhabilitación de cuatro a diez años para desempeñarse en otro empleo, puesto, cargo o comisión pública. De acuerdo con el artículo 211 bis 7, las penas previstas en este capítulo se aumentaran hasta en una mitad cuando se utilice la información en provecho propio o ajeno.

Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de informa-

ción que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Primer párrafo

Conducta	Modificar, destruir o provocar pérdida de información del Estado.
Bien Jurídico	La seguridad informática del Estado
Realización dolosa/ culposa	Sólo admite la realización dolosa por el criterio de numerus clausus

Sujeto Activo	Los sujetos autorizados para acceder al sistema o equipo.
Sujeto pasivo	El Estado
Objeto Material	Sistemas o equipos de informática del Estado
Circunstancias de tiempo, modo y lugar	No exige
Especiales medios de comisión	Al que estando autorizado para acceder a sistemas y equipos de informática del estado, indebidamente modifique, destruya o provoque perdida de información
Elementos subjetivos Específicos	En el tipo penal básico: No se establecen. En el tipo penal calificado: se utilice la información en provecho propio o ajeno.
Nexo causal	Delito de resultado que se traduce en la modificación, destrucción o perdida de la información del Estado
Elementos normativos	Persona autorizada Sistemas de informática del Estado. Equipos de informática del Estado. Mecanismo de seguridad del Estado. Indebidamente*
Sanción	Se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa. De acuerdo con el artículo 211 bis 7, las penas previstas aumentaran hasta en una mitad cuando se utilice la información en provecho propio o ajeno.

*Jorge Esteban Cassou Ruiz (2009): Tales ilícitos también pueden considerarse como un fin en tratándose del uso de computadoras, sobre todo cuando se trata de información de tipo industrial, en relación con el ordinal 211 Bis, de la ley del enjuiciamiento penal federal, la Primera Sala del más alto Tribunal de Justicia de la Nación, ha establecido de que el vocablo indebidamente empleado en dicho precepto legal, no provoca confusión; en primer lugar, porque es posible precisar su significado a través de su concepto gramatical y, el segundo, porque su sentido puede

fijarse desde el punto de vista jurídico y determinar cuando la conducta es indebida para considerarse delictuosa. Además, el hecho de que el Código Penal Federal no contenga un anunciado especial que desentrañe el significado de ese elemento normativo, lo cual se entiende por constituir un elemento de valoración jurídica, no implica infracción a la citada garantía, pues, se trata de un concepto cuyo contenido resulta claro tanto en el lenguaje común como en el jurídico. www.ijf.cjf.gob.mx/publicaciones/revista/28/Delitos_informáticos.pdf

Segundo párrafo

Conducta	Copiar información del Estado.
Bien Jurídico	La seguridad informática del Estado
Realización dolosa/ culposa	Sólo admite la realización dolosa por el criterio de numerus clausus
Sujeto Activo	Persona autorizada para acceder a la información.
Sujeto pasivo	El Estado
Objeto Material	Sistemas o equipos de informática del Estado
Circunstancias de tiempo, modo y lugar	De manera indebida.
Especiales medios de comisión	No exige
Elementos subjetivos Específicos	En el tipo penal básico: No se establecen. En el tipo penal calificado: se utilice la información en provecho propio o ajeno.
Nexo causal	Delito de conducta que vulnera la confidencialidad de la información.

Elementos normativos	Sistemas de informática del Estado. Equipos de informática del Estado.
Sanción	Se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa. De acuerdo con el artículo 211 bis 7, las penas previstas aumentaran hasta en una mitad cuando se utilice la información en provecho propio o ajeno.

Tercer párrafo

A quien estando autorizado para acceder a sistemas, equipos o medios de almacenamiento informáticos en materia de seguridad pública, indebidamente obtenga, copie o utilice información que contengan, se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública.

Conducta	Obtener, copiar o utilizar información en materia de seguridad pública.
Bien Jurídico	La seguridad informática de la seguridad pública
Realización dolosa/ culposa	Sólo admite la realización dolosa por el criterio de numerus clausus

Sujeto Activo	El sujeto autorizado.
Sujeto pasivo	El Estado
Objeto Material	Sistemas o equipos de informática del Estado
Circunstancias de tiempo, modo y lugar	De manera indebida.
Especiales medios de comisión	No exige.
Elementos subjetivos Específicos	En el tipo penal básico: No se establecen. En el tipo penal calificado: se utilice la información en provecho propio o ajeno.
Nexo causal	Delito de resultado que se traduce en la obtención, copia o utilización de información en materia de seguridad pública
Elementos normativos	Sistemas de informática de seguridad pública. Equipos de informática de seguridad pública. Medios de almacenamiento informáticos en materia de seguridad pública. Servidor público o exservidor público.
Sanción	Se le impondrá pena de cuatro a diez años de prisión y multa de quinientos a mil días de salario mínimo general vigente en el Distrito Federal. Si el responsable es o hubiera sido servidor público en una institución de seguridad pública, se impondrá además, hasta una mitad más de la pena impuesta, destitución e inhabilitación por un plazo igual al de la pena resultante para desempeñarse en otro empleo, puesto, cargo o comisión pública. De acuerdo con el artículo 211 bis 7, las penas previstas aumentaran hasta en una mitad cuando se utilice la información en provecho propio o ajeno.

Artículo 211 bis 4.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Primer párrafo

Conducta	Modificar, destruir o provocar pérdida de información de las instituciones que integran el sistema financiero.
Bien Jurídico	La seguridad de la información del sistema financiero.
Realización dolosa/ culposa	Sólo admite la realización dolosa por el criterio de numerus clausus
Sujeto Activo	Puede ser cualquier persona, no se establece calidad específica.
Sujeto pasivo	Las instituciones que integran el sistema financiero.
Objeto Material	Sistemas o equipos de informática

Circunstancias de tiempo, modo y lugar	Protegidos por un mecanismo de seguridad.
Especiales medios de comisión	Al que sin autorización.
Elementos subjetivos Específicos	En el tipo penal básico: No se establecen. En el tipo penal calificado: se utilice la información en provecho propio o ajeno.
Nexo causal	Delito de resultado que se traduce en la transformación o eliminación material de la información.
Elementos normativos	Sistemas de informática. Equipos de informática. Mecanismo de seguridad. Instituciones que integran el sistema financiero, de acuerdo la remisión del artículo 211 bis 6, señala que para los efectos de este artículo se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 bis del Código Penal Federal.
Sanción	Se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. De acuerdo con el artículo 211 bis 7, las penas previstas aumentaran hasta en una mitad cuando se utilice la información en provecho propio o ajeno.

Segundo párrafo

Conducta	Conocer o copiar la información.
Bien Jurídico	La seguridad informática del sistema financiero.
Realización dolosa/ culposa	Sólo admite la realización dolosa por el criterio de numerus clausus

Sujeto Activo	Puede ser cualquier persona, no se establece calidad específica.
Sujeto pasivo	Instituciones que integran el sistema financiero
Objeto Material	Sistemas o equipos de informática
Circunstancias de tiempo, modo y lugar	Protegido por un mecanismo de seguridad.
Especiales medios de comisión	Al que sin autorización.
Elementos subjetivos Específicos	En el tipo penal básico: No se establecen. En el tipo penal calificado: se utilice la información en provecho propio o ajeno.
Nexo causal	Delito de conducta que vulnera la confidencialidad de la información.
Elementos normativos	Sistemas de informática. Equipos de informática. Mecanismo de seguridad. Instituciones que integran el sistema financiero, de acuerdo la remisión del artículo 211 bis 6, señala que para los efectos de este artículo se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 bis del Código Penal Federal.
Sanción	Se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa De acuerdo con el artículo 211 bis 7, las penas previstas en este capítulo se aumentaran hasta en una mitad cuando se utilice la información en provecho propio o ajeno.

Artículo 211 bis 5.- Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

Primer párrafo

Conducta	Modificar, destruir o provocar pérdida de información de las instituciones que integran el sistema financiero.
Bien Jurídico	La seguridad de la información del sistema financiero.
Realización dolosa/ culposa	Sólo admite la realización dolosa por el criterio de numerus clausus
Sujeto Activo	Tipo básico: Persona autorizada para acceder. Tipo calificado: funcionarios o empleados de las instituciones que integran el sistema financiero.

Sujeto pasivo	Las instituciones que integran el sistema financiero
Objeto Material	Sistemas o equipos de informática
Circunstancias de tiempo, modo y lugar	No exige.
Especiales medios de comisión	No exige.
Elementos subjetivos Específicos	En el tipo penal básico: No se establecen.
Nexo causal	Delito de resultado que se traduce en la transformación o eliminación material de la información. En el tipo penal calificado: se utilice la información en provecho propio o ajeno, el resultado es que exista un beneficio con consecuencia de la acción a favor del activo o de un tercero.
Elementos normativos	Sistemas de informática. Equipos de informática. Mecanismo de seguridad Instituciones que integran el sistema financiero, de acuerdo la remisión del artículo 211 bis 6, señala que para los efectos de este artículo se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 bis del Código Penal Federal.
Sanción	Se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Las penas previstas incrementaran en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero. De acuerdo con el artículo 211 bis 7, las penas aumentarán hasta en una mitad cuando se utilice la información en provecho propio o ajeno.

Segundo párrafo

Conducta	Copiar información de las instituciones que integran el sistema financiero
Bien Jurídico	La seguridad de la información de las instituciones financieras.
Realización dolosa/ culposa	Sólo admite la realización dolosa por el criterio de numerus clausus
Sujeto Activo	Tipo básico: Persona autorizada para acceder a sistemas y equipos de informática de las instituciones financieras. Tipo calificado: funcionarios o empleados de las instituciones que integran el sistema financiero
Sujeto pasivo	Instituciones que integran el sistema financiero
Objeto Material	Sistemas o equipos de informática
Circunstancias de tiempo, modo y lugar	Indebidamente
Especiales medios de comisión	Al que estando autorizado
Elementos subjetivos Específicos	En el tipo penal básico: No se establecen.
Nexo causal	Delito de conducta que vulnera la confidencialidad de la información de las instituciones que integran el sistema financiero. En el tipo penal calificado: se utilice la información en provecho propio o ajeno, el resultado es que exista un beneficio con consecuencia de la acción a favor del activo o de un tercero.

Elementos normativos	Sistemas de informática. Equipos de informática. Mecanismo de seguridad. Instituciones que integran el sistema financiero, de acuerdo la remisión del artículo 211 bis 6, señala que para los efectos de este artículo se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 bis del Código Penal Federal.
Sanción	Se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Las penas previstas incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero. De acuerdo con el artículo 211 bis 7, aumentarán hasta en una mitad cuando se utilice la información en provecho propio o ajeno.

9.1-Delitos especiales previstos en la ley Federal de proteccion de datos personales en posesion de particulares[30].

Esta ley es de reciente expedición y protege los datos personales que se encuentran en poder de particulares, contempla los delitos que más adelante se mencionan y de los que haremos el análisis de sus elementos para precisar cuáles son los elementos críticos de su configuración y el bien jurídico tutelado.

[30]Lucia Villafranca (2014), sostiene que la legislación mexicana, se vio influida por el contenido de la Ley Orgánica de Protección de Datos personales de España, aun cuando el legislador español no incluyó un capitulo penal en la Ley de referencia.

El objeto de esta Ley es la protección de los datos personales en posesión de los particulares, contiene disposiciones para regular su tratamiento, control e información y garantizar la privacidad de las personas; su propósito esencial es la protección de la privacidad o el derecho a la intimidad de las personas, cuestión que tendremos presente en el momento de hacer la interpretación gramatical, sistemática y teleológica del capítulo penal que nos mueve, para verificar si en su caso, la técnica de construcción de los tipos penales en efecto responde a este objetivo o puede provocar consecuencias en su aplicación por la ambigüedad de su texto.

A este respecto Irene Navarro Frías (2012) sostiene que:

> el bien jurídico protegido por estos artículos de la ley, es la intimidad, entroncando así con lo dispuesto en al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. Que aunque la LFPDPPP al exponer la finalidad de la misma se refiera expresamente a la privacidad y al derecho a la autodeterminación informativa de las personas, ambas nociones se hallan comprendidas en un concepto de intimidad entendido como aquellas manifestaciones de la personalidad individual o familiar cuyo conocimiento o desarrollo quedan reservados a su titular o sobre las que ejerce alguna forma de control cuando se ven implicados terceros.

Un aspecto fundamental de esta legislación, es que, como hemos apuntado, el derecho se ha visto obligado a configurar una norma de protección de elementos que han surgido en la sociedad de la información, en este caso los

denominados datos personales, que se acumulan en bases de datos, mismos que son tratados y gestionados por diversos sujetos del ámbito privado tanto personas físicas como jurídicas, y que en los casos previstos suponen un calidad de garante de información que por su carácter sensible impone su protección penal.

Aspecto medular en la interpretación de esta norma penal especial, son las remisiones al reglamento de la citada ley, y además el aspecto de consentimiento previo del titular de la información personal y la información de los denominados derechos ARCO[31], así como el conocimiento de la orientación del legislador en el capítulo administrativo sancionador donde se prevén una serie de comportamientos que determina cuál es la dirección de la protección de la información que persigue.

La descripción de la conducta prohibida establecida en el artículo 67, se centra en la vulneración de la seguridad de las bases de datos, y su diseño se encamina a la protección de este aspecto, éste es definido por el artículo 19 en los siguientes términos:

> Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Los

[31]Derechos Arco: Acceso, rectificación, corrección y oposición respecto de la información personal.

> responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico.

El concepto normativo de seguridad es amplio ya que no sólo se refiere a los aspectos de la seguridad lógica, que en este caso los asimila a las técnicas, sino a la seguridad física y agrega una más de carácter administrativo, lo que amplia considerablemente los supuestos, además no hay exigencia en esta hipótesis típica de afectación del bien jurídico tutelado que es el derecho humano de la intimidad.

En el artículo 68 cuando establece como conducta núcleo del tipo penal, el tratar datos personales, nos encontramos con la técnica de los delitos penales en blanco, cuando el legislador hace una remisión para encontrar los límites de la prohibición, ya que para llenar de contenido el verbo tratar, nos tenemos que remitir a lo previsto en la fracción que define en el mismo ordenamiento lo que es tratamiento, que dice *Tratamiento*: La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

En la ampliación de la remisión, nos encontramos que el concepto de transferencia se encuentra definido en el mismo artículo 3, fracción XIX, éste lo describe como toda

comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento, lo que indica una técnica legislativa inapropiada en el caso de este capítulo penal de la ley, que pudiera dar lugar a cuestionamiento sobre la inseguridad jurídica que provocan para los gobernados.

El diseño que observamos en estos tipos penales implica que la conducta delictiva se agota con la vulneración de la seguridad de las bases de datos personales independientemente que se afecte o no el derecho a la intimidad de la persona que se trate.

Para interpretar sistemáticamente el capítulo penal en los casos de la naturaleza de los datos personales, tendremos que considerar lo previsto por el artículo segundo de esta ley, que precisa los siguientes conceptos:

Datos personales: Cualquier información concerniente a una persona física identificada o identificable.

Datos personales sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

CAPÍTULO XI
De los Delitos en Materia del Tratamiento Indebido de Datos Personales

Artículo 67.- Se impondrán de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.

Artículo 68.- Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.

Artículo 69.- Tratándose de datos personales sensibles, las penas a que se refiere este Capítulo se duplicarán.

Análisis dogmático

Artículo 67.- Se impondrán de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.

Conducta	Provocar una vulneración de seguridad a las bases de datos bajo su custodia.

Bien Jurídico	La intimidad de las personas
Realización dolosa/ culposa	Sólo admite la realización dolosa por el criterio de numerus clausus
Sujeto Activo	Al particulares que estando autorizado para tratar datos personales y además tenga su custodia, con excepción de los previsto en al art. 2 de dicha Ley Federal.
Sujeto pasivo	Puede ser cualquier persona, no se establece calidad específica.
Objeto Material	Bases de datos independientemente del soporte electrónico o papel
Circunstancias de tiempo, modo y lugar	Una vulneración de seguridad
Especiales medios de Comisión	No exige
Elementos subjetivos específicos.	Con ánimo de lucro
Nexo causal	La conducta de vulneración supone la afectación de la seguridad de las bases de datos bajo su custodia.
Elementos normativos	Datos personales. (art 3 fracción V de LFPDPPP) Seguridad de las bases de datos. Bajo su custodia. Datos personales sensibles (art 3 fracción VI de LFPDPPP)
Sanción	Se le impondrán de tres meses a tres años de prisión. En el tipo agravado Tratándose de datos personales sensibles, la pena se duplicará.

Artículo 68.- Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del

error en que se encuentre el titular o la persona autorizada para transmitirlos.

Conducta	Tratar datos personales para transmitirlos.
Bien Jurídico	La seguridad de la información de datos personales. La privacidad de la personas identificadas o identificables
Realización dolosa/ culposa	Sólo admite la realización dolosa por el criterio de numerus clausus
Sujeto Activo	Cualquier persona.
Sujeto pasivo	Puede ser cualquier persona, no se establece calidad específica.
Objeto Material	Datos personales, contenidos en diversos soportes no solo electrónicos sino en soporte papel (ficheros).
Circunstancias de tiempo, modo y lugar	
Especiales medios de Comisión	Mediante el engaños y aprovechamiento del error.
Elementos subjetivos específicos.	Fin de lucro indebido.
Nexo causal	La conducta de tratar, supone la manipulación de los datos personales e implica un resultado de transformación de los mismos.
Elementos normativos	Datos personales. Transmisión. Persona autorizada. Tratamiento. (Art 3 fracción XVII de LFPDPPP)
Sanción	Se le impondrán de seis meses a cinco años. En el tipo agravado Tratándose de datos personales sensibles, la pena se duplicará.

9.2-Codigo Penal del Estado de Chiapas

En el Código Penal del Estado de Chiapas se incluyó, siguiendo la misma técnica legislativa, un capítulo de delitos propiamente informáticos, en la misma forma que el Código Penal Federal, se le denominó de manera semejante delitos de acceso ilícito, aun cuando en su configuración se hicieron algunos ajustes, que hay precisar y comentar sus consecuencias para su interpretación y aplicación.

Advertimos que el legislador no delimita, si los supuestos de estos delitos son de mera conducta o también se incluyen supuestos de riesgo, ya sea concreto o abstracto, lo que provoca un problema de inseguridad jurídica que no observa el principio de legalidad previsto en el artículo 14 de la Constitución Política de los Estados Unidos Mexicanos, respecto a su descripción utiliza conceptos informáticos que implican una remisión que podrían provocar el problema de los tipos penales en blanco; además utiliza una reiteración que puede dar lugar a equívocos, cuando señala que "quien ingrese sin estar autorizado y sin derecho, o lo haga innecesariamente", en ese caso se planteará el supuesto de que cuando será necesaria la realización de esas conductas.

En el caso de Chiapas establece como requisitos de procedibilidad el hecho de que se necesita querella de parte ofendida, lo que implica reconocer en cierta medida que tutela un bien jurídico individual, ya que sólo podrán formularla el particular agraviado y los representantes legales

de las dependencias públicas. Podría entonces considerarse que en el caso de Chiapas el legislador no le concede al bien jurídico tutelado el reconocimiento de su carácter macro colectivo y se excluyen sus hipótesis de peligro.

CAPÍTULO II
ACCESO ILÍCITO A SISTEMAS DE INFORMÁTICA

Artículo 439.- Al que sin autorización modifique, destruya, o provoque pérdida de información contenida en sistemas o equipo de informática protegidos por algún mecanismo o sistema[32] de seguridad o al que no tenga derecho a accesar, se le impondrá una sanción de uno a cuatro años de prisión y de cuarenta a doscientos días multa.

Al que, estando autorizado o tenga derecho de acceso a los sistemas o equipo de informática protegido por algún mecanismo o sistema de seguridad, innecesariamente o en perjuicio de otro destruya, modifique, o provoque pérdida de información que contengan los mismos, la pena prevista en el párrafo anterior, se aumentará en una mitad.

Artículo 440.- Al que, sin autorización accese, modifique, copie, destruya o provoque pérdida de información contenida en sistema o equipo de informática de alguna de-

[32]Agrega la distinción entre mecanismo y sistema de seguridad. En el federal solo refiere a mecanismo, en el caso local se agrega que pudiera ser un sistema de seguridad, habrá que localizar dentro de la normatividad de la materia informática del estado esta diferencia.

pendencia pública protegida por algún sistema o mecanismo de seguridad se le impondrá una sanción de dos a seis años de prisión y de doscientos a seiscientos días de multa.

Artículo 441.- Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, innecesariamente o en perjuicio de otro o del servicio público modifique, destruya o provoque pérdida de información que contengan se impondrá prisión de tres a ocho años y de trescientos a ochocientos días multa.

Artículo 442.- Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, sin autorización copie, transmita o imprima información que contengan se le impondrá de uno a cuatro años de prisión y de cien a trescientos días multa.

Artículo 443.- Los delitos previstos en este título serán sancionados por querella de parte ofendida.

Análisis desglosado

Artículo 439.- Al que sin autorización modifique, destruya, o provoque pérdida de información contenida en sistemas o equipo de informática protegidos por algún mecanismo o sistema de seguridad o al que no tenga derecho a accesar, se le impondrá una sanción de uno a cuatro años de prisión y de cuarenta a doscientos días multa.

Conducta	Modificar, destruir o provocar perdida.
Bien Jurídico	La información y su seguridad informática
Realización dolosa/ culposa	Sólo admite la realización dolosa por el criterio de numerus clausus
Sujeto Activo	Cualquier particular que no tenga derecho de acceso.
Sujeto pasivo	Puede ser cualquier persona, no se establece calidad específica.
Objeto Material	Equipo o sistema de informática
Circunstancias de tiempo, modo y lugar	Protegidos por algún mecanismo o sistema de seguridad.
Especiales medios de Comisión	No exige
Elementos subjetivos específicos.	
Nexo causal	
Elementos normativos	Sistema o equipos de informática. Seguridad de las bases de datos. Mecanismo de seguridad. Sistema de seguridad.
Sanción	De uno a cuatro años de prisión y de cuarenta a doscientos días multa.

Segundo párrafo

Al que, estando autorizado o tenga derecho de acceso a los sistemas o equipo de informática protegido por algún mecanismo o sistema de seguridad, innecesariamente o en perjuicio de otro destruya, modifique, o provoque pérdida de información que contengan los mismos, la pena prevista en el párrafo anterior, se aumentará en una mitad.

Conducta	Destruir, modificar o provocar perdida de información
Bien Jurídico	La información y la seguridad informática
Realización dolosa/ culposa	Sólo admite la realización dolosa por el criterio de numerus clausus
Sujeto Activo	Al particular autorizado y que tenga derecho de acceso.
Sujeto pasivo	Puede ser cualquier persona, no se establece calidad específica.
Objeto Material	Equipo o sistema de informática
Circunstancias de tiempo, modo y lugar	En perjuicio de otro o innecesariamente.
Especiales medios de Comisión	No exige
Elementos subjetivos específicos.	
Nexo causal	Delito de resultado, ya que la conducta debe de ser idónea para destruir, modificar o provocar la pérdida definitiva de la información.

Elementos normativos	Seguridad de las bases de datos. Mecanismo de seguridad. Sistema de seguridad. Equipo o sistema de informática.
Sanción	La pena de uno a cuatro años de prisión y de cuarenta a doscientos días multa, se aumentará en una mitad

Artículo 440.- Al que, sin autorización accese, modifique, copie, destruya o provoque pérdida de información contenida en sistema o equipo de informática de alguna dependencia pública protegida por algún sistema o mecanismo de seguridad se le impondrá una sanción de dos a seis años de prisión y de doscientos a seiscientos días de multa.

Conducta	Accese, modifique, copie, destruya o provoque perdida de la información
Bien Jurídico	La información y la seguridad informática
Realización dolosa/ culposa	Sólo admite la realización dolosa por el criterio de numerus clausus
Sujeto Activo	Al particular no autorizado
Sujeto pasivo	Dependencia pública.
Objeto Material	Equipo o sistema de informática
Circunstancias de tiempo, modo y lugar	En perjuicio de otro o innecesariamente.

Especiales medios de Comisión	No exige
Elementos subjetivos específicos.	
Nexo causal	Delitos de mera conducta, en las hipótesis de acceso y copia, y de resultado en los supuestos de la modificación, destrucción o pérdida de la información.
Elementos normativos	Seguridad de las bases de datos.
Sanción	De dos a seis años de prisión y de doscientos a seiscientos días de multa.

Artículo 441.- Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, innecesariamente o en perjuicio de otro o del servicio público modifique, destruya o provoque pérdida de información que contengan se impondrá prisión de tres a ocho años y de trescientos a ochocientos días multa.

Conducta	Modifique, destruya o provoque perdida
Bien Jurídico	La información o la seguridad informática
Realización dolosa/ culposa	Sólo admite la realización dolosa por el criterio de numerus clausus
Sujeto Activo	Al particular autorizado y que tenga derecho de acceso.

Sujeto pasivo	Dependencia Pública.
Objeto Material	Información en equipo o sistema de informática
Circunstancias de tiempo, modo y lugar	En perjuicio de otro o innecesariamente.
Especiales medios de Comisión	No exige
Elementos subjetivos específicos.	
Nexo causal	Delito de resultado
Elementos normativos	Seguridad de las bases de datos. Dependencia pública.
Sanción	De tres a ocho años y de trescientos a ochocientos días multa

Artículo 442.- Al que estando autorizado para acceder a sistemas y equipos de informática de alguna dependencia pública, sin autorización copie, transmita o imprima información que contengan se le impondrá de uno a cuatro años de prisión y de cien a trescientos días multa.

Conducta	Copiar, trasmitir o imprimir.
Bien Jurídico	La información y la seguridad informática

Realización dolosa/ culposa	Sólo admite la realización dolosa por el criterio de numerus clausus
Sujeto Activo	Al particular autorizado y que tenga derecho de acceso.
Sujeto pasivo	Puede ser cualquier persona, no se establece calidad específica.
Objeto Material	Información en equipo o sistema de informática
Circunstancias de tiempo, modo y lugar	En perjuicio de otro o innecesariamente.
Especiales medios de Comisión	No exige
Elementos subjetivos específicos.	
Nexo causal	Delito de resultado
Elementos normativos	Seguridad de las bases de datos. Equipos o sistemas de informática. Dependencia pública.
Sanción	De uno a cuatro años de prisión y de cien a trescientos días multa.

CONCLUSIONES

1.- La política criminal en al ámbito informático, responde a lineamientos, principios y criterios marcados por instituciones internacionales y los estados nacionales replican en sus respectivas legislaciones estas directrices, con sus respectivos matices y muchas veces con deficiencias en

técnica legislativa, lo que provoca algunas confusiones en el momento de convenir sobre los conceptos doctrinales derivados de la aparición del nuevo campo de estudio del derecho penal informático.

2.- La orientación del poder punitivo del Estado como una expresión del control social formal, internaliza la idea de que los criminales informáticos son personas físicas con finalidades lúdicas que amenazan la seguridad informática, desde una perspectiva económica de la información y por ello en el denominado control social de reacción materializa una serie de conductas que las normas nacionales tutelan como prioridad de las cuestiones de seguridad del Estado y las instituciones financieras. Aspecto que deberá de replantearse principalmente a orientar la función penal hacia la protección de los derechos humanos que se ponen en riesgo en la sociedad de la información.

3.- La tendencia creciente de los roles sociales en entornos cibernéticos y los nuevos conflictos derivados, justifican la intervención del Estado mediante el poder punitivo, para generar un proceso expansivo del derecho penal, sin agotar otras instancias para resolverlos. Convierte al derecho penal informático tanto en lo formal como en lo material, en un área de riesgo para los derechos humanos de los gobernados en sus respectivos países.

4.- En algunos casos, la aparición de conductas tipificadas se orientan a la protección de derechos subjetivos fundamentales, como es el de la protección de intimidad de

las personas. En estos casos comparto esa tendencia de intervención punitiva, exclusivamente a los casos dolosos y graves, efectivamente necesarios cuando otras vías de intervención no hayan sido eficaces para hacer efectivo del derecho penal mínimo de un estado democrático de derecho.

5.- El debate sobre la existencia de una doctrina del derecho penal informático y sobre la nomenclatura de los delitos de la denominada sociedad de la información, es solamente de carácter conceptual en el ámbito de la doctrina nacional e internacional, lo que puede generar confusiones en los casos de interpretación y aplicación de los casos concretos, si no se comprende que el ejercicio sistemático dentro del campo de la dogmática penal específica, responde al análisis de una realidad delimitada. Esto es, en el caso de México su legislación federal en materia de delitos relacionados con las nuevas tecnologías de la informática y las comunicaciones responde a la armonización internacional pero se ajustan al estilo y modo de construir su sistema jurídico desde la perspectiva de la seguridad y complica las funciones e interpretación y aplicación de estos supuestos y pone en riesgo derechos subjetivos, desde esta perspectiva deberán de abordarse, para encontrar la solución justa y legal en el momento indicado, teniendo en cuenta la teología de la norma y el contexto en que se aplica siempre respetando los principios de presunción de inocencia, legalidad, lesividad del bien jurídico y culpabilidad entre otros.

6.- En estricto sentido los delitos informáticos en México, se encuentran tipificados en el capítulo segundo del título noveno del Código Penal Federal, el cual contiene otra serie de figuras relacionadas con las tecnologías de la información y la comunicación o con el entorno del usos de los medios electrónicos, que no caben en esta categoría, porque el bien jurídico directo que protegen no es preponderantemente la seguridad informática como en estos casos, y los delitos previstos en la Ley Federal de Protección de Datos en posesión de particulares protegen los datos personales y con ello la dignidad de las personas que son titulares de ellos.

7.- Este estudio no se alinea al proceso de expansión del derecho penal y su endurecimiento con el incremento de la penas, por el contrario pretende exhibir los riesgos de esa tendencia nacional e internacional, y reflexiona sobre la necesidad de la identificación de los auténticos autores de la cibercriminalidad, así como de aplicar una política criminal de dos velocidades como lo propone Silva Sánchez, y desde la perspectiva de protección esencial de los bienes jurídicos que suponen el respeto de los derechos humanos.

8.- Sobre el complejo tema de los bienes jurídicos penalmente protegidos en los delitos informáticos, sostenemos que en efecto deberá considerarse la tutela del interés macrocolectivo de la seguridad de la información estratégica y clave para el adecuado funcionamiento de la sociedad, pero que por eso mismo y con el propósito de que esa

protección no se convierta en mecanismo de control social para las clases desprotegidas, se ponderé con exactitud el campo de intervención del derecho penal y los destinarios de las medidas de prevención y de sanción penal, y que no se abuse de la técnica de los delitos de riesgo para ampliar el uso de poder punitivo del Estado.

9.- En el diseño actual de los delitos en México, no se encuentran explícitamente hipótesis de peligro concreto o abstracto, aunque para algunos autores la forma en que están construidos - en el caso de los delitos de la ley Federal de Protección de Datos personales en posesión de particulares - contiene riesgo abstracto a la intimidad, como si es posible apreciar en otros códigos penales de otros países, pero su construcción adolece de principio de taxatividad y pone en riesgo el principio de legalidad.

10.- Serán los jueces como constructores del derecho, los que tendrán que definir los contornos de intervención del poder penal del estado, ante un diseño legal como el que revisamos y ante la compleja diversidad de casos que no puede predecir el legislador y por ello, utilizó formas muy abiertas en la confección de los tipos penales. Lo que puede dar lugar a cuestionar su constitucionalidad.

LA SEGURIDAD INFORMÁTICA EN LA FUNCIÓN NOTARIAL

INTRODUCCIÓN

He advertido la necesidad de analizar el impacto que ha tenido el desarrollo de las Tecnologías de la Información y Comunicación (TIC's) en el ámbito de la función notarial. Por ello este estudio se propone revisar algunas de las implicaciones que en materia de seguridad informática y protección de los derechos personales se presentan en la aplicación de estas tecnologías en las actividades del notario de corte latino.

El grado de desarrollo tecnológico en los diversos países puede tener diferencias en razón de sus capacidades económicas, no obstante, los efectos de este suceso tecnológico son constantes y relevantes para apuntarlos en una monografía; por tal motivo, en esta ocasión nos ocuparemos de los casos de España y México.

Este estudio no pretende describir completamente, ni agotar el análisis del marco jurídico que regula el tema, únicamente se referirá a las cuestiones relacionadas con la

administración segura de la firma electrónica; así como de la protección de los datos de las personas en la actividad notarial.

Empero, pretende ser un análisis que visualice y ponga de manifiesto los problemas de la seguridad informática relacionada con el derecho a la privacidad y a la autodeterminación informativa en estos ámbitos; así como los medios de seguridad que deberán de gestionar los notarios públicos por la constante influencia de las tecnologías de la informática y las comunicaciones en su actividad primordial. Hace un ejercicio prospectivo acerca de las nuevas funciones notariales relacionando el desarrollo e incorporación de las TIC´s.

1.- LA SOCIEDAD DE LA INFORMACIÓN Y LA FUNCIÓN DEL NOTARIO PÚBLICO DEL SISTEMA LATINO

En las últimas décadas, la comunicación humana se ha transformado de manera acelerada, en virtud de la evolución de las tecnologías de la informática[1] y de las telecomunicaciones. Este fenómeno global ha sido calificado, desde distin-

[1]El empleo de la Informática en el ámbito jurídico se remonta a finales de los años cincuenta, época en que se comienzan a utilizar las computadoras no sólo con fines matemáticos sino también lingüísticos, sufriendo un proceso de transformación impresionante en pocas décadas.

tos ángulos, con el nombre de "Sociedad de la Información" (Reusser, 2003)[2], su rasgo fundamental es el avance tecnológico en la digitalización[3] de la información, lo que permite guardarla en grandes volúmenes (Ribagorda,1996) y su desplazamiento casi instantáneo. En estos tiempos, mucha información pasa por las computadoras e Internet; es decir, existe un uso masivo de dichos medios, característica esencial de este momento de desarrollo de la sociedad.

Las características de la sociedad de la información se manifiestan en los cambios que se han gestado en todos los órdenes de la vida, ésta se desarrolla de diferente forma y sus actores se transforman. El ámbito jurídico no se ha escapado de este fenómeno y la actividad de los fedatarios públicos tampoco. Por ello, muchas instituciones educativas que forman profesionales del derecho, han incorporado en los distintos niveles de estudio, los cursos de derecho informático e informática aplicada al derecho en los programas de estudio de posgrado. En derecho notarial el tema de la in-

---

[2]En los últimos quince años, y especialmente en la década de los noventa, ha cobrado auge y difusión nacional y mundial el concepto de "Sociedad de la Información" (SI), sobre todo por su gran promoción en el ámbito de las políticas públicas, utilizándose de mejor o de peor manera para referirse, en general, a cualquier cuestión derivada de innovaciones tecnológicas que han devenido en un cambio en el modelo social.

[3]Según Lynch (1996) "Cuando se habla de la era digital se refiere a algo que ya afecta y afectará mucho más la vida humana hasta los planos más recónditos: la vida institucional, la economía, la cultura, la información, los entretenimientos. Todo estará digitalizado: desde los actos más nimios hasta los más trascendentes del hombre como su nacimiento, la vida intrauterina, el registro de su nacimiento o su casamiento, sus propiedades, sus transacciones, su salud, sus entretenimientos, su desarrollo espiritual y cultural".

formática notarial será progresivamente más relevante. Los profesionales del derecho, del presente y del futuro, no se conciben sin el dominio de las habilidades y competencias informáticas (Ribagorda, 2000)"[4].

Afirma Juan José Ríos Estavillo (1997), que la relación entre el Derecho y la Informática no es unilateral[5] ya que sigue dos líneas, por un lado los aspectos normativos del uso de la Informática desarrollados bajo el Derecho de la Informática[6] y, por otro, la que nos interesa para este estudio, la aplicación de la Informática en la recuperación de análisis y tratamientos jurídicos y, en particular, de la información notarial.

Para los efectos de este trabajo se precisan conceptos básicos de esta disciplina jurídica, nos referimos, a la Informática Jurídica, que de acuerdo con Julio Téllez Valdés (2010), es "la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de información

[4]Arturo Ribagorda (2000) señala que uno los aspectos de la vulnerabilidad de los sistemas informáticos es la falta de capacitación o inexperiencia de los usuarios en el manejo de los instrumentos informáticos.

[5]Entre el Derecho y la Informática se destacan, entre otros, dos tipos de interrelaciones. Si se toma como enfoque el aspecto netamente instrumental, se está haciendo referencia a la Informática Jurídica. Pero al considerar a la Informática como objeto del Derecho, se hace alusión al Derecho de la Informática o simplemente Derecho Informático.

[6]Es el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la Informática.

jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación".

La informática jurídica ha sido clasificada para su estudio en diversas vertientes según su desarrollo, en un primer momento se presentó en los términos de creación y recuperación de información que contenía datos jurídicos o relacionados a ellos, por lo que se le denominó Informática Documentaria, la cual dio paso a la Informática de Control y Gestión, misma que engloba los ámbitos jurídico – administrativo, judicial, registral y despachos de abogados y notarías y, por último, la Informática Jurídica Metadocumentaria o también llamada Sistemas Expertos Legales, la cual brinda apoyo en la toma de decisiones, educación, investigación, redacción y previsión del Derecho, sin embargo ninguna es excluyente ya que pueden coexistir simultáneamente.

Es la segunda de ellas, la Informática Jurídica de Control y Gestión, la mayormente utilizada en las diversas oficinas jurídicas, entre ellas, las relacionadas con la actividad notarial, siendo los primeros profesionales del derecho que advirtieron la utilidad de la informática de gestión, incluso en la época en que tal avance constituía una novedad costosa y era juzgada por muchos como una extravagancia modernista (SCJN, 2006), esta área también es conocida como "Ofimática Notarial, siendo su objetivo primordial llevar a cabo el seguimiento de trámites y procesos notariales, tales como fichero de clientes; base de datos personales; consulta

de legislación; jurisprudencia y bibliografía; índice de documentos; contabilidad y tratamiento de textos" (SCJN, 2006, p. 33); todo con la finalidad de mantener actualizada la información y llevar un buen control de la misma.

Las funciones relacionadas a la actividad notarial van más allá del simple tratamiento de textos; son varios los procedimientos notariales que se hacen dependiendo de estas herramientas y se avizoran muchos otros, como es el caso de las ventanillas únicas virtuales, la gestión de documentos electrónicos, la firma digital y sus distintos usos en los diversos actos jurídicos.

Por otra parte, una característica importante del sistema notarial latino que prevalece tanto en España como en México es que el notario público es considerado un profesional del Derecho que tiene la facultad de expedir documentos que ofrezcan certeza jurídica y que signifiquen una herramienta jurídica de suma trascendencia, por ello el valor probatorio pleno otorgado por las diversas legislaciones procesales a tales instrumentos. La fe pública delegada por el Estado y envestida en el notario de corte latino otorga plena autenticidad a las declaraciones emitidas o hechos presenciados por un notario, así como a los actos celebrados ante él, modelo prevaleciente en ambas latitudes como un sistema de prevención de conflictos judiciales. Hoy en día, el Notario Público deberá trasladar esta seguridad jurídica que ha venido plasmando en el mundo del soporte papel al documento o soporte electrónico.

> En cuanto al elemento medular de la función notarial del sistema latino que es el documento notarial, este descansa sobre cuatro bases jurídicas que son, al mismo tiempo, su propia esencia, a saber:
>
> 1. El documento notarial es producto del pensamiento humano.
> 2. El documento notarial es un hecho jurídico (o acto jurídico).
> 3. La autoría del documento notarial corresponde al notario y reside en él.
>
> 4. El documento notarial, en su autenticidad, da fe pública."[7]

En el sistema notarial latino se evidencia, mediante la importancia de la autoría del documento por parte del notario, el papel principal que desempeña en el mundo jurídico de la vida social, la autoría del documento por parte del notario y su control de la legalidad lo distingue de otras formas documentales en que la actividad del profesional se limita a la legitimación o autenticación de la firma (como el notary public). Por eso, al notario latino se le exige el conocimiento adecuado y científico del derecho; sin embargo, los tiempos actuales también le exigen adaptar dichas funciones al desarrollo de las TIC's con todo y sus implicaciones jurídicas.

El procedimiento de fe pública notarial es el instrumento que permite a los ciudadanos modular sus contratos

[7]Bases o principios fundamentales del sistema del notariado latino Consejo Permanente de La Haya Holanda. Aprobado por el Bureou de la CCNI el l8 de enero de 1986 y por el Consejo Permanente de La Haya, 13, 14 y 15 marzo 1986.

y dar carácter de documento público a sus declaraciones de voluntad en el ámbito de las transacciones jurídicas. El documento notarial tiene la virtud de tener calidad probatoria, de poseer la capacidad de ejecutabilidad y, en consecuencia, generar la seguridad jurídica que requieren tanto los ciudadanos como las empresas.

Hoy en día, en la práctica notarial mexicana, es normal y necesario el uso de las computadoras, que han sustituido en gran medida a las máquinas de escribir cualquiera que sea su modalidad; así como la utilización obligada del Internet para la elaboración de los instrumentos notariales, la búsqueda de leyes y jurisprudencia por medio de la web o de medios ópticos, como los cd's o dvd's; la obtención de permisos para la constitución de sociedades ante la Secretaría de Economía y su inscripción en el Registro Público de Comercio; la tramitación de certificados de libertad o gravamen en el Registro Público de la Propiedad; el cálculo y entero de impuestos en las enajenaciones; la tramitación de cédulas catastrales ante la Dirección de Catastro Urbano y Rural dependiente de la Secretaría de Hacienda local, además de las diversas declaraciones y avisos ante el Servicio de Administración Tributaria, y ya que desde que entró en vigor el acuerdo A/078/13 del Procurador General de la República el cual entró en vigencia el 17 de julio de 2013, el cual abroga el Acuerdo A/327/12 por el que se creó la Coordinación General de Información y Análisis Financiero, para convertirse en la Unidad Especializada en Análi-

sis Financiero de la Procuraduría General de la República (PGR) que actualmente se encuentra en funciones. Todos estos procesos que, de una u otra forma, son llevados a cabo, a través del uso de las TIC´s.

Por tal motivo, independiente a la necesidad de capacitación para el ingreso a la institución notarial, es obligación del notario, el continuo estudio, preparación y actualización, sobre todo sí se considera la constante transformación que las instituciones jurídicas presentan y mucho más por el impacto que los cambios científicos y tecnológicos tienen en el ámbito de las normas jurídicas (Pérez, 2000) .

Mario Lozano, en su obra los Grandes Sistemas Jurídicos (1982) considera que la historia del Derecho está condicionada por las tres revoluciones; la de la escritura, la de la imprenta y la de la ordenación electrónica de datos; tenemos pues, que estar de acuerdo con el planteamiento de este paradigma. La revolución tecnológica cibernética ha modificado los patrones de comportamiento y progresivamente estamos viviendo los de la ofimática notarial, lo que impone capacitación y adiestramiento permanente a los titulares y colaboradores de las notarías públicas.

El uso de los avances de la Informática ha disminuido los tiempos de respuesta en los servicios notariales, los obstáculos burocráticos se han eliminados en cierta medida. Se tienen ahora mayores y mejores herramientas para agilizar la función notarial. Es conveniente comentar, desde otra perspectiva, que se han presentado nuevos inconvenientes

informáticos que aunque menores, han generado impactos en la prestación de los citados servicios, como es el caso de la caída de los sistemas o la deficiente operación del algún software, o la contaminación por virus del sistema o red interna o, en su caso, la falta de capacitación del personal; pero todo ello demuestra la interdependencia de lo jurídico con lo informático, y la necesidad de políticas de seguridad informática en los despachos notariales.

La modernización permanente de los equipos informáticos así como de los programas de las oficinas notariales y la capacitación del recurso humano que trabaja en las mismas, sobre cuestiones de derecho informático y, por ende, en informática jurídica y derecho de la informática, es una de las vías estratégicas para mejorar la función notarial y sus retos futuros, para poder competir con servicios de calidad ante los demás fedatarios públicos que se incorporan paulatinamente al mercado de servicios de esta naturaleza.

El diseño de programas de cómputo adecuados al marco jurídico del país en materia de cálculo de impuestos federales y estatales, la determinación de presupuestos respetando aranceles, la realización de los tramites registrales y catastrales y otros temas del quehacer cotidiano de las notarías se resolverán, sin duda, con el auxilio de la ofimática notarial, que en un futuro no muy lejano, organizará su gestión administrativa con el diseño de software específico a necesidades concretas.

2.- IMPORTANCIA DE LA SEGURIDAD INFORMÁTICA EN LA PRÁCTICA NOTARIAL

Así como se hizo referencia a la sociedad de la información o del conocimiento, en amplio sentido, debemos precisar, para los efectos de este segmento, que existe también un criterio que identifica a la sociedad posmoderna como sociedad de riesgo[8], en donde el tema de la seguridad cobra una dimensión sobresaliente. Así, por ejemplo, se han clasificado los ámbitos de seguridad como sigue:

> 1º. Seguridad Técnica, que permita obtener comunicaciones privadas, auténticas e íntegras inter-partes y que garantice que los sitios están a salvo de piratas informáticos o "hackers".
>
> 2º. Seguridad Jurídica, entendiendo por tal, un marco jurídico regulador de las eventuales responsabilidades que pueden dimanar de conductas o actos ilícitos a través de la red.
>
> 3º. Seguridad mercantil o económica, que sería la aplicación del concepto anterior para garantizar un marco seguro de transacciones financieras a través de la red.
>
> 4º. Seguridad a los consumidores, evitando el abuso de las

[8]Ulrich Beck (1994) en su libro La sociedad del riesgo. Hacia una nueva modernidad, Paidós, Barcelona. 1994. desarrolló el concepto de la sociedad de riesgo a partir de la aparición de los avances de las ciencias de la electrónica y las telecomunicaciones, subrayando como uno de los rasgos de la sociedad posmoderna, el de la revolución microlectrónica: "junto con la desindustrialización, esta transformación plantea una nueva forma filosófica de entender el trabajo, el sexo, relaciones sociales, estrato socio-económico y formas de producción. Es la superación definitiva de la industrialización clásica".

> grandes empresas de su posición de dominio y la utilización de cláusulas abusivas" (Alfin, 2009).

Sin adentrarnos en la teoría sobre la sociedad de riesgo y sobre el ámbito teórico general de la seguridad, nos interesa dejar establecido que en este contexto se ha desarrollado todo un sistema de seguridad informática que consiste básicamente en garantizar el patrimonio físico y lógico de los recursos del sistema de información (material informático o programas) de una organización, para que éstos sean utilizados de la manera que se decidió y que el acceso a la información contenida en los equipos, así como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

En amplio sentido se entiende a la seguridad informática como la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable. En estricto sentido la seguridad informática se entiende como un estado protegido de la información contenida en un sistema que se encuentra con baja probabilidad de peligro, daño o riesgo. Se admite como peligro o daño informático toda aquella amenaza que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo.

Para la mayoría de los expertos en informática, el concepto de seguridad absoluta en este ámbito es prácticamente imposible, se admite que siempre tendrá un porcentaje de

vulnerabilidad. No obstante, se ha convenido que existen condiciones normales de un sistema seguro cuando se reúnan las siguientes características:

1. Integridad: La información sólo puede ser transformada por quien está autorizado y bajo controles.
2. Confidencialidad: La información sólo puede ser consultada por los autorizados.
3. Disponibilidad: Ser protegida pero lista para su uso por los autorizados.
4. Irrefutabilidad (No repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción" (Téllez, 2003).

Dependiendo de las fuentes de amenaza, la seguridad puede dividirse en seguridad lógica y seguridad física. La primera se refiere a la protección de los diversos programas informáticos y, la segunda, a los equipos y recursos que despliegan a los primeros, esto se logra a través de la *criptografía* (Carreño y Moreno, 2002)[9].

En estos momentos, la seguridad informática es un tema de dominio obligado por cualquier usuario de Inter-

[9]Carreno y Moreno (2002) comentan que la criptografía se divide en dos grandes ramas, la criptografía de clave privada o simétrica y la criptografía de clave pública o asimétrica.

net[10], para no permitir que su información sea comprometida, tal es el caso de la función notarial.

A diferencia del principio jurídico, en materia de seguridad informática se dice que lo que no está permitido debe estar prohibido. Por lo anterior, se establecen una serie de medidas, como son las siguientes:

1. Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.

2. Garantizar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).

3. Asegurar que se utilicen los datos, archivos y programas correctos en y por el procedimiento elegido.

4. Tener la certeza de que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.

5. Controlar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.

6. Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien esta-

[10] _____ sostienen que "desde el mismo momento en que surge la iniciativa en una organización de conectarse a una red pública como Internet, deben comenzar a evaluarse no solo los beneficios sino también los riesgos. Cualquier tipo de actividad en la que se utiliza "la red" está expuesta a una serie de amenazas, ya sea por la vulnerabilidad de la información que intercambiamos por medio de ella o por la posibilidad de ser atacados dentro de nuestra propia casa, surgiendo la necesidad de aplicar mecanismos cada vez más ingeniosos para protegernos".

blecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.

7. Mantener actualizadas las contraseñas de accesos a los sistemas de cómputo (Téllez, 2003).

Todas estas reglas deberán de ser aplicadas dentro de la organización del despacho notarial para establecer un sistema seguro de manejo de la información utilizada para el desarrollo de las funciones, lo que supone el apoyo de expertos en la materia y el conocimiento en conceptos de informática jurídica.

3.- EVOLUCIÓN DEL MARCO JURÍDICO EN ESPAÑA Y MÉXICO SOBRE SEGURIDAD INFORMÁTICA Y FUNCIÓN NOTARIAL

Este ejercicio, como señalamos en un principio, no será exhaustivo, simplemente referiremos los aspectos más sobresalientes regulados en este ámbito con el propósito de ilustrar que el tema de la seguridad informática debe ser conocido por los operadores y responsables de un despacho notarial, quienes deberán brindar en el mundo digital la misma garantía de seguridad e identidad jurídica que en la actualidad ofrece el mundo de papel.

La Constitución Española de 1978, en el artículo 18.4 establece que: “La ley limitará el uso de la informática para

garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". La Ley Orgánica 5/1992, de 29 de Octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), ahora derogada, fue la primera ley española que reguló de forma específica la materia, su ámbito de aplicación se limitaba a los ficheros de carácter automatizados. En su lugar fue publicada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal que tiene por objeto, "garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar"; con la que se cumplieron los requisitos establecidos por la Directiva Europea 95/46/CE del Parlamento Europeo y del Consejo, de 24 de Octubre de 1995, relacionado con la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de los mismos.

Posteriormente, se emite el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, relativo a la protección de datos de carácter personal, mismo que, según lo determinado en su exposición de motivos, "comparte con la Ley Orgánica, la finalidad de hacer frente a los riesgos que para los derechos de la personalidad pueden suponer el acopio y tratamiento de datos personales"

Por su parte, el Real Decreto 994/1999 (LORTAD), regulaba las medidas técnicas y organizativas que debían aplicarse a los sistemas de información que trataran datos de carácter personal de forma automatizada.

En España, la Ley Orgánica de Protección de Datos o también llamada LOPD y su normativa de desarrollo, se ocupa exclusivamente de asegurar los derechos de acceso a los datos y recursos con las herramientas de control y mecanismos de identificación. Estos mecanismos permiten saber que los operadores tienen sólo los permisos que se les dio.

La política de seguridad, que esta ley recomienda se basa en:

- Elaborar reglas y procedimientos para cada servicio de la organización.
- Definir las acciones a emprender y elegir las personas a contactar en caso de detectar una posible intrusión.
- Sensibilizar a los operadores con los problemas ligados con la seguridad de los sistemas informáticos.

Los derechos de acceso de los operadores deben ser definidos por los responsables jerárquicos y no por los administradores informáticos, los cuales tienen que conseguir que los recursos y derechos de acceso sean coherentes con la política de seguridad definida. Además, como el administrador suele ser el único en conocer perfectamente el sistema, tiene que derivar a la directiva cualquier problema e información relevante sobre la seguridad y eventualmente aconsejar estrategias a poner en marcha, así como ser el

punto de entrada de la comunicación a los trabajadores sobre problemas y recomendaciones en término de seguridad.

Por su parte, la Directiva 99/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica establece las bases para proporcionar a los Estados miembros un marco jurídico para la firma electrónica, el cual no afectará al régimen jurídico de otras formalidades no contractuales y cuyo régimen jurídico aplicable será el establecido por cada país[11].

En España, la Sentencia 292/2000, de 30 de noviembre, tras desvincular el derecho a la protección de datos del derecho a la intimidad, señala que "el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso", añadiendo que "estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacena-

[11] *Ídem*.

miento y tratamiento, así como su uso o usos posibles, por un tercero".

En el mismo sentido, consideramos conveniente mencionar los aspectos más significativos de la evolución histórica del marco jurídico mexicano, respecto de la protección de datos, firma electrónica y seguridad informática.

Mayo 2000. Se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor, así como de Ley Federal de Procedimiento Administrativo: reformas relevantes en la materia, en virtud de la aceptación del medio electrónico como elemento válido para la manifestación del consentimiento de los contratantes, su utilización en caso de que el acto requiera forma escrita, y la estipulación de la facultad conferida al fedatario público para generar, archivar, recibir o comunicar la información con los términos en que las partes han decidido obligarse a través de dichos medios; así mismo el reconocimiento con carácter de prueba de la información que conste en medios electrónicos; la automatización del Registro Público de Comercio y su operación a través de un sistema, ahora denominado SIGER; y de especial importancia, para este análisis, destacar el precedente que el legislador marcó en cuanto a protección de datos personales, con la reforma a la Ley Federal de Protección al Consumidor, al señalar la obligación

del proveedor de resguardar y hacer buen uso de la información proporcionada por el consumidor a través del uso de medios electrónicos, y enumerar los derechos de éste respecto de la misma.

Noviembre 2001. Conservación de Mensajes de Datos NOM-151. En ella se establecen los requisitos que deben observarse para la conservación de mensajes de datos.

Abril 2003. Ley de Firmas Electrónicas. Agosto 2003 Se reforman y adicionan diversas disposiciones del Código de Comercio, en materia de Firma Electrónica. Se estipulan criterios de neutralidad tecnológica, compatibilidad internacional y equivalencia funcional entre el Mensaje de Datos con la información documentada en medios no electrónicos y de la Firma Electrónica con la firma autógrafa, en cuanto a comercio electrónico y se dota al notario o corredor público de facultades para prestar servicios de Certificación relacionados con firmas electrónicas, estableciendo que para tal efecto, deberá contar con elementos suficientes para garantizar la seguridad y confidencialidad de la información, factor de especial relevancia y a tomar en cuenta en cuanto a la protección de datos personales.

Enero 2004. Factura Electrónica. Se declara que las personas que tengan certificado de firma electrónica avanzada y lleven su contabilidad en sistema electrónico, podrán emitir comprobantes en documento digital y con sello digital, debiendo incorporar en los documentos los requisitos de identificación establecidos en el Código Fiscal de la Federación.

Julio 2004. "Reglamento del Código de Comercio en Materia de Prestadores de Servicio de Certificación. Se establecen las disposiciones y los requisitos técnicos y jurídicos para darse de alta y para operar como Prestador de Servicios de Certificación en el sector comercial" (Durán, 2007).

Diciembre 2005. Procedimientos Administrativos por medios electrónicos. Se establecen las disposiciones que deberán observar las dependencias de la Administración Pública Federal, para la recepción de promociones y resoluciones administrativas definitivas a través de medios de comunicación electrónica.

Agosto de 2006. Acuerdo Interinstitucional por el que se establecen los lineamientos para la homologación, implantación y uso de la firma electrónica avanzada en la Administración Pública Federal.

Junio 2009. Se adiciona un segundo párrafo al artículo 16 de la Constitución Política, para garantizar el derecho de toda persona a la protección de sus datos personales.

Julio 2010. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. El objetivo de esta ley fue garantizar el adecuado resguardo y tratamiento de datos personales en posesión de particulares.

Enero 2012. Ley de la Firma Electrónica Avanzada. En esta ley se establecen los parámetros generales para la aceptación y uso de la firma digital en el país, definiéndose las instancias a cargo de las cuales estarán los procesos relacionados con los sectores mercantil, financiero y gubernamental.

Enero de 2014. El uso obligatorio de la factura electrónica. A partir del 01 de enero de 2014 todos los contribuyentes deben emitir factura electrónica, excepto las personas físicas cuyos ingresos durante 2012 no hayan excedido de 500 mil pesos, quienes tienen tres meses más (es decir tienen enero, febrero y marzo) para migrar a este esquema.

El artículo 14, de la Ley de la Firma Electrónica Avanzada mencionada en líneas precedentes, establece que: El responsable velará por el cumplimiento de los principios de protección de datos personales, debiendo adoptar las medidas necesarias para su aplicación. Lo anterior aplicará aún y cuando estos datos fueren tratados por un tercero a solicitud del responsable. El encargado deberá tomar las medidas necesarias y suficientes para garantizar que el aviso de privacidad dado a conocer al titular, sea respetado en todo momento por él o por terceros con los que guarde alguna relación jurídica.

Esta legislación ubica al notario como un particular que da tratamiento a los datos de sus clientes, le obliga a realizar el aviso de privacidad, que le impone incluso tener colocado en lugar visible del despacho notarial. Por otro lado tiene el deber de informar que en caso de se vea obligada o necesite transferir su información personal a terceros nacionales o extranjeros distintos de las autoridades administrativas y judiciales para el cumplimiento de los servicios notariales, informará al particular previamente de esta situación a efecto de solicitarle autorización e infor-

marle sobre el destinatario o tercero receptor y finalidades de dichas transferencias, en términos de los previsto en los artículos 36 y 37 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y 68 de su Reglamento. Finalmente hay que considerar que esta Ley, impone criterios de seguridad informática, no sólo obligaciones con relación a clientes y usuarios, sino también respecto a los datos personales de trabajadores y otro tipo de información, entre otros.

Ahora bien, en lo que se refiere a la automatización notarial en México, habrá que remitirnos a la Ley del Notariado del Estado de Jalisco, misma que en el Título Segundo, Capítulo Segundo, Sección Segunda, artículo 76 al 82 bis, define al protocolo electrónico, como el conjunto de documentos, implementos y archivos electrónicos en que constan los hechos y actos autorizados por el notario por ese medio, los libros que se formen con la impresión de ellos, sus índices y actas de apertura y cierre"[12], asimismo, establece como elemento imprescindible del mismo la firma electrónica certificada del notario y, en su caso, de los otorgantes.

Por último, a nivel internacional, encontramos la siguiente legislación relativa al comercio electrónico, misma que deberá ser analizada y adoptada, no únicamente por los miembros de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), sino adecuarla a

[12]Consultar artículo 76 de la Ley del Notariado para el Estado de Jalisco.

la función notarial para satisfacer las necesidades tanto nacionales como internacionales sobre firma digital.

• 2005. Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales, cuya finalidad es fomentar la seguridad jurídica y la previsibilidad comercial cuando se utilicen comunicaciones electrónicas en la negociación de contratos internacionales.

• 2001. Ley Modelo de la CNUDMI sobre las firmas electrónicas, la cual ha sido creada para dotar de mayor certeza jurídica al empleo de la firma electrónica.

• 1996. Ley Modelo de la CNUDMI sobre Comercio Electrónico, que permite facilitar el empleo de los modernos medios de comunicación y de archivo de la información, y

• 1985. Recomendación sobre el valor jurídico de la documentación informática, dirigida a las autoridades públicas y a las organizaciones internacionales que trabajan en la preparación de textos jurídicos reguladores del comercio, con la sugerencia de que se revise la normativa aplicable, en el ámbito de su respectiva competencia, del procesamiento automático de datos, con objeto de eliminar todo obstáculo innecesario que dificulte su empleo en el comercio internacional[13].

[13] *Ibídem*, p. 37 y 38.

4.- FIRMA ELECTRÓNICA Y FUNCIÓN NOTARIAL

La firma tradicionalmente cumple con las funciones siguientes: "individualiza al autor del documento de tal forma que no admite duda, manifiesta su aceptación para hacer suyos los efectos jurídicos de determinado acto, evita la posible repudiación de parte del documento y, por último, modifica el contenido del documento" (Trueba, 2007).

El Real Decreto – ley 14/1999, de 17 de septiembre, publicada en España sobre firma electrónica la define como "el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge."

Algunas publicaciones sobre función notarial, definen a la firma electrónica "como el conjunto de datos electrónicos puestos y enviados de computadora a computadora donde el firmante (emisor) asocia al texto electrónico enviado (mensaje de datos) para servir de medio de identificación del firmante y asegurar que el firmante reconoce y aprueba la información contenida en ese mensaje de datos y que tiene el mismo valor jurídico y procesal que la firma autógrafa" (Galván, 2012, p.171)

Es importante señalar que el uso de la firma electrónica ha trascendido a tal grado que es posible firmar una demanda de amparo con el uso de la misma siempre y cuando se cumplan con los requisitos establecidos por la Ley que

la regula, es menester precisar que en estos casos es conocida como FIREL (Firma Electrónica Certificada por el Poder Judicial de la Federación)[14] y deberá ser la misma que se registra ante el Poder Judicial de la Federación tal como lo establece la tesis aislada común con número de registro 2010386: "DEMANDA DE AMPARO DIRECTO. SI SE PRESENTA MEDIANTE EL USO DE UNA FIRMA ELECTRÓNICA DISTINTA DE LA REGULADA POR EL CONSEJO DE LA JUDICATURA FEDERAL (FIREL), AQUÉLLA NO PUEDE TENER EL EFECTO DE SER EQUIVALENTE A LA AUTÓGRAFA, PARA LA PROCEDENCIA DEL JUICIO."[15]

El término firma electrónica se refiere al conjunto de datos electrónicos que identifican a una persona en específico, normalmente va adjunta al documento que se transmite por medios telemáticos, es la señal electrónica equivalente a la firma tradicional[16] y manuscrita. Su objetivo es asegurar al receptor la personalidad del emisor del mensaje, garanti-

[14]"¿Cuáles son los beneficios de contar con la FIREL?", Consejo de la Judicatura Federal, 25 de enero de 2016, en https://www.cjf.gob.mx/documentos/TripticoFIREL.pdf

[15]Tesis XIX.1o.A.C.2 K (10a.), Semanario Judicial de la Federación y su Gaceta, Décima Época, t. IV, Libro 24, Noviembre de 2015, p. 3485.

[16]La ausencia de firma autógrafa, genera cierto rechazo ante la incomprensión de la seguridad del sistema, este rechazo social a la utilización de estos instrumentos, cuya raíz es la inseguridad. Inseguridad ante la identidad del destinatario y del receptor del mensaje; inseguridad en cuanto a la veracidad y autenticidad del contenido del mensaje; inseguridad en cuanto a su validez como documento probatorio, es ahí cuando surge la firma electrónica avanzada y la posible intervención del notario como entidad certificadora.

za de cierto modo que éste no ha sido alterado o modificado. Es ahora, también, un instrumento de identificación electrónica del notario en diversas actuaciones ante las entidades públicas, en materia fiscal y registral que se aparta de las clásicas como el sello de autorizar y la firma autógrafa.

Fernando Ramos Suárez (1999), dice que la firma electrónica consiste en el uso de un método de encriptación, el cual puede ser llamado asimétrico o de clave pública, dicho método, nos explica el mencionado autor, radica en crear dos claves asociadas, las cuales pertenecerán a un sujeto, una de dichas claves será pública y otra privada, lo anterior quiere decir que la clave pública será conocida por diferentes personas, mientras tanto la privada únicamente la sabrá el sujeto a que antes hicimos mención, de esta forma cuando se pretenda enviar un mensaje de manera segura a dicho sujeto, se habrá de encriptar[17] el mensaje, con la clave pública del sujeto, para que únicamente éste, por medio de la clave privada, pueda descifrar lo contenido en el mensaje (Ramos, 2009).

Tanto en España como en México la normativa prevé dos tipos de firmas electrónicas: la básica y la avanzada.

La firma electrónica básica está compuesta de un conjunto de datos recogidos de forma electrónica que formalmente identifican al autor y se incorporan al propio do-

[17]Encriptar: (anglicismo). Encriptar es la acción de proteger información para que no pueda ser leída sin una clave. Sinónimos de Encriptar: cifrar, codificar, extraído de. http://www.alegsa.com.ar/Dic/encriptar.php

cumento, pero este modelo informático adolece de cierta debilidad. No hay certeza plena respecto de los datos enviados, es decir no hay seguridad de que hayan sido creados por la persona que lo firma o que verdaderamente lo ha firmado él y no una tercera persona que lo suplanta.

Para contrarrestar la mencionada debilidad es que se creó la firma electrónica avanzada, a la que nuestros ordenamientos reconocen valor probatorio[18]. Este modelo de firma electrónica permite la identificación cierta del emisor

[18]FIRMA ELECTRÓNICA AVANZADA. EL HECHO DE QUE EL CÓDIGO FISCAL DE LA FEDERACIÓN NO ESTABLEZCA SU DEFINICIÓN NO VIOLA LA GARANTÍA DE LEGALIDAD. El artículo 17-D del Código Fiscal de la Federación establece que cuando las disposiciones fiscales obliguen a presentar documentos, éstos deberán ser digitales y contener una firma electrónica avanzada del autor, salvo los casos previstos en el propio precepto, y que para esos efectos deberá contarse con un certificado que confirme el vínculo entre un firmante y los datos de creación de una "firma electrónica avanzada", expedido por el Servicio de Administración Tributaria cuando se trate de personas morales y por un prestador de servicios de certificación autorizado por el Banco de México cuando se trate de personas físicas, mediante el cumplimiento de ciertos requisitos, entre ellos, el de la comparecencia del interesado o de su apoderado o representante legal en caso de personas morales, con la finalidad de acreditar su identidad. De lo anterior se concluye que no se viola la garantía de legalidad contenida en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, por el hecho de que el Código Fiscal de la Federación no establezca una definición particular de lo que debe entenderse por "firma electrónica avanzada", pues del indicado numeral 17-D se advierte el propósito perseguido con ésta, el cual, además de identificar al emisor de un mensaje como su autor legítimo, como si se tratara de una firma autógrafa, garantiza la integridad del documento produciendo los mismos efectos que las leyes otorgan a los documentos con firma autógrafa, teniendo el mismo valor probatorio; lo anterior, en razón de que la firma electrónica avanzada está vinculada a un certificado expedido por una autoridad, en este caso, por el Servicio de Administración Tributaria, en el que constan los datos del registro respectivo. Amparo en revisión 262/2007. Radio XEAGS, S.A. de C.V. 13 de junio de 2007. Cinco votos. Ponente: Sergio Salvador Aguirre Anguiano. Secretario: Óscar Zamudio Pérez.

Segunda Sala de la Suprema Corte de Justicia de la Nación. Semanario Judicial de la Federación y su Gaceta. Novena Época. Tomo XXVI, Agosto de 2007, Tesis: 2a. XCVII/2007, p. 638, No. Registro IUS: 171757.

del mensaje ya que está vinculada de manera única al que firma el documento y a los datos que incorpora, debido a que es el signatario quien únicamente tiene el control exclusivo de estas claves, además de que permite saber sí estos datos han sido modificados posteriormente o en su trayecto.

El ordenamiento español anteriormente referido señala que la firma electrónica avanzada "es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos".

Gradualmente, la firma electrónica se está usando en el sector privado, para contratación por medios electrónicos, así como en la diversas operaciones que ahora caracterizan al creciente comercio electrónico. Es útil, además, para realizar actuaciones en el ámbito de la Administración Pública, tanto para las relaciones entre los propios organismos como para las que sostiene con el ciudadano, como es el caso de las declaraciones fiscales y los trámites sobre historias registrales de propiedad, por mencionar algunos. En el ámbito notarial mexicano, a manera de ejemplo, se utiliza para rendir declaraciones de las operaciones realizadas y que tienen incidencia fiscal mediante el programa denominado Declaranot.

En este punto es conveniente identificar los principios bajo los cuales podrá utilizarse la firma electrónica avanza-

da, según lo determinado por la Ley de Firma Electrónica Avanzada para el Estado de Chiapas:

> a) Neutralidad, implica utilizar cualquier tecnología sin que se favorezca alguna en particular;
>
> b) Equivalencia funcional, la firma electrónica avanzada se equipara a la firma autógrafa y un mensaje de datos a los documentos escritos;
>
> c) Autenticidad, ofrece la certeza de que un mensaje de datos ha sido emitido por el Firmante y por lo tanto le es atribuible su contenido y las consecuencias jurídicas que del mismo se deriven por ser expresión de su voluntad;
>
> d) Conservación, un mensaje de datos posee una existencia permanente y es susceptible de reproducción;
>
> e) Confidencialidad, es la característica que existe cuando la información permanece controlada y es protegida de su acceso y distribución no autorizada; y
>
> f) Integridad, se considera que el contenido de un mensaje de datos es íntegro cuando ha permanecido completo e inalterado, con independencia de los cambios que hubiere podido sufrir el medio que lo contiene, como resultado del proceso de comunicación, archivo o presentación.

Los dos tipos de firma son ya utilizados en el ámbito notarial en nuestros respectivos países, insisto, fundamentalmente en el ámbito de las funciones registrales y las cuestiones fiscales que realiza el notario como coadyuvante de la función fiscalizadora del Estado.

En España, por su parte, encontramos las entidades de certificación, que son personas o entidades que cumplen una serie de requisitos legales y que deben ser autorizados por el Ministerio de Justicia para otorgar certificados que acrediten que la persona o entidad que usa dicha firma es ciertamente quien dice ser. Las principales autoridades de certificación acreditadas son:

1. Agencia de Certificación Electrónica (ACE), está homologada por Visa y Mastercard y ofrece certificados para Entidades y Corporaciones dentro de comercio electrónico y de comunicaciones a través de Internet. (www.ace.es)

2. Fundación para el Estudio de la Seguridad de las Telecomunicaciones (FESTE), se trata de una entidad formada por registradores, notarios, abogados, la Universidad de Zaragoza e Intercomputer S.A. y su principal actuación se dirige a la contratación privada. (http://web.dit.upm.es/~enrique/ce/sec5/par512.html)

3. Certificación Española (CERES), es una entidad de certificación pública que lleva a cabo la Fábrica Nacional de Moneda y Timbre. Su campo de actuación es la garantía de seguridad, validez y eficacia de comunicaciones entre los órganos de la Administración Pública y entre las personas físicas y jurídicas que se relacionen con ella, sin olvidar servicios de Comunidades Autónomas, Entidades Locales y de derecho público siendo necesario únicamente un convenio previo.(www.cert.fnmt.es).

En España la prestación de estos servicios es libre, si

bien existe un procedimiento voluntario, que es la acreditación, mediante la cual la Administración, realizando las evaluaciones técnicas de rigor, emite una resolución o documento oficial donde certifica que ese prestador cumple con las normas de calidad y seguridad establecidas en cuanto a sus procedimientos, productos y tecnología que utiliza.

El papel de las Autoridades de Certificación consiste en recoger la declaración de voluntad del titular de una firma digital, asumiendo la obligación de quedar obligado por aquellos documentos cuya firma pueda ser comprobada mediante el uso de una llave pública determinada (Trueba, 2007, p. 87) .

Como podemos observar el notario está incluido como una entidad de certificación de clave pública y, por tanto, deberá de tener nociones de seguridad informática y criptografía y los conocimientos necesarios para entender cómo opera la firma electrónica avanzada.[19]

Ahora bien, la autoridad certificante tiene como objetivo primordial:

- Constatar si la clave pública pertenece a la persona quien dice ser su titular, por medio de la identificación física realizada con anterioridad a la certificación del par de claves.

[19]Entonces, una autoridad certificadora será la tercera parte en el intercambio entre una determinada clave pública y su propietario real. Actuando a manera de notario electrónico que extiende un certificado de claves, el cual está firmado con su propia clave, para así garantizar la autenticidad de dicha información.

- Certificar el procedimiento de identificación.
- Publicar la clave pública en un registro especial.
- Administrar el proceso en general de manera que implique una revisión periódica del proceso de identificación y verificación.
- Proceder a la inmediata publicación de toda causa de extinción, suspensión, revocación o modificación de clave pública (Trueba, 2007, p.87-88).

Aunque de manera tardía, México se ha sumado al proceso de legalizar y darle viabilidad a la firma electrónica; el 29 de agosto de 2003[20], se estableció el antecedente más importante en esta materia al marcar una actualización en la legislación mexicana en relación con la forma como las nuevas tecnologías han modificado el derecho mercantil y la interacción en la sociedad. Es menester precisar la firma Electrónica ya se encuentra regulada bajo la Ley de Firma Electrónica Avanzada que entró en vigor años más tarde el 11 de enero de 2012, así como su reglamento que entró en vigor hasta el 21 de marzo de 2014.

Sin embargo, pese a las reformas en los códigos civiles, procesales, de comercio[21] (Cornejo, 2001) y fiscales,

[20]Consultar Decreto por el que se reforman y adicionan diversas disposiciones del Código de Comercio en Materia de Firma Electrónica. Diario Oficial de la Federación. Viernes 29 de Agosto de 2003.

[21]Valentino Cornejo (2001) opina que aunque es verdad que en las reformas al Código de Comercio no se menciona expresamente a la firma electrónica como

prevalece una incertidumbre al omitir de las regulaciones una figura como la firma electrónica avanzada única para todas las operaciones, no sólo las tributarias y el órgano de control federal. Hasta ahora, la firma electrónica avanzada es empleada por la Secretaría de Hacienda y Crédito Público; la Secretaría de la Función Pública la usa para efectuar las declaraciones patrimoniales de los funcionarios de la Administración Pública Federal; por su parte, los Registros Públicos de Comercio la operan con el propósito de que sus empleados capturen información en el programa de cómputo de gestión de registros públicos (SIGER); además, las dependencias de la Administración Pública así como los notarios y corredores públicos pueden emitir certificados de firmas electrónicas, principalmente de aquéllas empleadas en el extranjero.

En síntesis, "con las reformas y adiciones a diversas leyes, que fueron publicadas en el Diario Oficial de la Federación el 29 de mayo pasado y más recientemente el 18 de septiembre, las operaciones de comercio electrónico en México ya disponen de un soporte legal, dado que en dichas reformas se reconoce no sólo el valor jurídico de los documentos electrónicos y la equivalencia de la firma electrónica con la firma autógrafa, sino que incluso reconocen la participación de los

forma de firmar a los documentos electrónicos, de manera perfecta podemos aplicar el artículo 90 del capítulo Del Comercio Electrónico en el Código de Comercio, la Firma Electrónica consiste en la utilización de un método de encriptación llamado asimétrico o de clave pública.

Notarios y Corredores Públicos en los proceso de emisión de certificados digitales y la obligatoriedad de su incorporación al Registro Público de Comercio" (Cornejo, 2001).

En México, el certificado expedido por el prestador del servicio podrá garantizar frente a terceros su integridad y su origen, aunque supuestamente deja sin resolver el problema de la identidad de la autoridad de certificación; sin embargo, las reformas al Código de Comercio contemplan, este supuesto, integrando la participación del fedatario público cuando para aquellos actos jurídicos en que sea necesaria la fe pública del notario deberá constar en instrumento público conforme con la legislación aplicable en la actividad notarial, aquí surge una nueva dimensión del notariado mexicano en el que aparecen dos nuevos conceptos informáticos como es el notario cibernético y el protocolo electrónico.

La intervención de particulares usando la firma electrónica y los actos notariales que la impliquen, son aspectos que se mencionan como un ejemplo más de la prospectiva que tendrá en lo futuro este instrumento de la informática jurídica en el ámbito del trabajo notarial, como lo es el testamento otorgado por medios electrónicos, empleando, por supuesto, la firma electrónica. Por ello, el manejo de ésta por parte del notario público requiere de conciencia en las implicaciones de su mal uso, sobre todo cuando éste otorga las claves a terceras personas, pues dicho acto se equipara a delegar su firma autógrafa.

5. DERECHO A LA INTIMIDAD, SECRETO PROFESIONAL Y FUNCIÓN NOTARIAL

La aplicación de los avances de la informática en el ámbito notarial ha supuesto una ostensible mejora de la productividad laboral, aumento de la capacidad de recolección de datos y de importante ajuste en la organización del despacho notarial. Sin embargo, su uso implica nuevos riesgos, en lo cualitativo, con relación a la protección de los datos personales[22] y, en consecuencia, del derecho a la intimidad y a la privacidad de los usuarios de los servicios notariales incluyendo el llamado derecho a la autodeterminación informativa.

El derecho a la intimidad[23] y el *Habeas Data*[24] está normado ya en algunos países, España y México lo tienen. Esta legislación protege el derecho de toda persona a su intimidad, a su buen nombre, y a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los

[22]Cualquier información concerniente a personas físicas identificadas o identificables.

[23]Este derecho consiste en la facultad que tiene cada persona, de disponer de una esfera, ámbito privativo o reducto infranqueable de libertad individual, el cual no puede ser invadido por terceros, ya sean particulares o el propio Estado, mediante cualquier tipo de intromisiones, las que pueden asumir muy diversos signos.

[24]Derecho que asiste a toda persona identificada o identificable a solicitar judicialmente la exhibición de los registros públicos o privados en los cuales se hallan incluidos sus datos personales o los de su grupo familiar, para tomar conocimiento de su exactitud, y requerir la rectificación, la supresión de datos inexactos u obsoletos que impliquen discriminación.

bancos de datos y en archivos de entidades públicas y privadas, sin embargo, en el caso de México esto último se limitaba únicamente a las entidades públicas, al menos en materia federal hasta el 2010 que se extendió a los particulares que manejen datos personales. El derecho supone que en la recolección, tratamiento y circulación de datos personales se respetarán la libertad y demás garantías relacionadas con la intimidad y privacidad de sus titulares, considerando las restricciones en torno al marco de acción del Estado, como es el caso de cuestiones de seguridad nacional, seguridad pública, bienestar económico, defensa del orden, prevención del delito, protección de la salud así como la protección de los derechos de los demás.

Así pues, en la actualidad, según la naturaleza de su contenido, podemos hablar dos tipos de bancos de datos o archivos, a saber:

1. Archivos públicos en poder del Estado. Las autoridades y los organismos encargados generalmente de condensar y capturar esa información, son: el Instituto Federal Electoral, el INEGI, los registros civiles, catastros, entre otros.

2. Archivos privados, manejados por terceros, por ejemplo: los datos que conservan las empresas y los particulares (Bailón, 2005).

Sólo mediante el acceso a estos bancos de datos el individuo puede saber en qué medida está controlado (dere-

cho a informarse), o bien, rechazar ese control por considerarlo abusivo (derecho a anulación o cancelación), así como hacerlo veraz (derecho de corrección) (Morales, 1984) .

A nivel internacional, este derecho se ha recogido en diversos ordenamientos concretando con ello la protección de la intimidad y del honor de la persona en el tratamiento de sus datos, tal es el caso de la Declaración Universal de los Derechos Humanos, la Declaración Americana de los Derechos y Deberes del Hombre y; entre los países que han regulado este tópico encontramos a España con la Ley Orgánica 15/1999 sobre la Protección de Datos de Carácter Personal, referida con antelación; Alemania; Francia en su Ley relativa a la Informática, Archivos y Libertades; Estados Unidos con su Privacy Acta o Ley de la Privacidad; Canadá en la Human Rights Act o Ley de Derechos Humanos y; por su parte, México reconoce este derecho a través de la Ley de Transparencia y Acceso a la Información Pública Gubernamental, publicada en el Diario Oficial de la Federación el 11 de junio de 2002 (Morales, 1984) y últimamente y de manera más concreta con la Ley fFederal de Protección de Datos Personales en Posesión de los Particulares publicada en el Diario Oficial de la Federación el 5 de julio de 2010.

Los dos últimos ordenamientos citados son reglamentarios de lo previsto en los artículos 6 y 16[25] de la Cons-

[25]Villanuevay Nucci (2012, p.9) comentan:.. "El derecho de acceso a la información pública tiene como complemento esencial la protección de los datos personales. En México, al artículo 6 y el 16 de la Constitución Política de los Estados Unidos

titución que señala que "toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros". Se consagran dos derechos que la función notarial debe tener presentes, el derecho de protección de los datos personales y el derecho del particular a la autodeterminación informativa[26].

Incluso el artículo 67 configura un delito en materia del Tratamiento Indebido de Datos Personales, que contempla como bien jurídico tutelado a la seguridad informática, estableciendo que: Se impondrán de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.

Mexicanos garantizan la protección de los datos personales como un derecho humano".

[26]DIRECTRICES PARA LA ARMONIZACIÓN DE LA PROTECCIÓN DE DATOS EN LA COMUNIDAD IBEROAMERICANA. En el punto 7. Seguridad y confidencialidad en el tratamiento, señala sobre el tema de la seguridad informática, que es aplicable a la función notarial.

7.1. Deberán adoptarse las medidas técnicas y organizativas que resulten necesarias para proteger los datos contra su adulteración, pérdida o destrucción accidental, el acceso no autorizado o su uso fraudulento.

7.2. Quienes 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 su relación con el titular del archivo de datos.

En México, la seguridad informática es un bien jurídico protegido por las leyes penales, tanto federales[27] como estatales[28], este régimen incluye la responsabilidad del manejo incorrecto que haga el notario o los empleados de la notaría respecto a la información contenida en sus archivos electrónicos. De igual manera en España existen normas penales que tutelan este bien jurídico.

Abordar el tema del secreto profesional y la función notarial, ya sea en cuanto al notario mismo, sus colaboradores o a los registros, pudiera parecer como algo inapropiado; ya que por lo común se parte de la idea que el propio concepto de la función indica una orientación contraria (notario público, registros públicos) (Vidal, 2002). Todo hace suponer que no puede existir privacidad (protección de la vida privada) y que todo es abierto al conocimiento público. ¿Cómo una escritura pública puede ser materia de secreto profesional? Aquí es donde el derecho de uso conforme al fin y de la interconexión de archivos[29] adquiere un papel de suma trascendencia.

No obstante la reflexión anterior, secreto profesional y derecho a la intimidad, elementos importantísimos en el

---

[27]Consultar Libro segundo, Título Noveno, Capítulo Segundo, del Código Penal Federal.

[28]Consultar Libro segundo, Título Décimo Noveno, Capítulo segundo, del Código Penal para el Estado de Chiapas.

[29]Tales derechos, junto con el de acceder, el de rectificar, el de cancelar y el de oponerse, conforman el derecho a la protección de datos personales los cuales son conocidos como Derechos ARCO.

ejercicio de la función notarial y la atención personalizada, son hoy más vulnerables y más difíciles de guardar a causa de la mayor participación de profesionales del derecho y de la informática en la toma de decisiones; de la evolución y modernización de las instituciones fiscales, notariales y registrales; así como de la aplicación de las nuevas tecnologías por la constitución de bancos de datos en los que se tiene información detallada de las personas que usan los servicios notariales.

El secreto profesional asume la tutela de valores individuales, como la dignidad de la persona y la protección de su intimidad, y de valores sociales, como el bien común y la protección del inocente o de daños a terceros. Esto implica la necesidad del dominio y conocimiento de los mecanismos de seguridad informática en el ámbito notarial para evitar el mal uso de dicha información y el criterio para entregar la información sobre las personas a las autoridades judiciales y registrales sólo cuando sea procedente conforme a la ley y respeto del secreto profesional.

Sin embargo, aunque el secreto profesional tiene límites como los valores sociales y el orden público, algunas veces este conflicto entre intereses requiere de una adecuada valoración en el manejo de esta información individual. Los profesionales deben ser conscientes de cómo manejar el secreto profesional en el ejercicio de su función ante una sociedad de la información, en donde las posibilidades de romperlo son distintas.

El derecho a la intimidad salvaguarda todos los aspectos que configuran la historia biográfica de una persona, su salud[30], sus bienes, su voluntad, datos personales sensibles[31], entre otros, que se alojan de manera electrónica en el protocolo del notario y que al sistematizarse pueden ser utilizados de manera inadecuada, ya que se encuentran en los instrumentos notariales por la formalidad que exige su configuración y siendo cruzados pueden construir perfiles para distintos fines, por ello es fundamental que deben de estar custodiados eficientemente por el titular del despacho notarial, esto constituye el deber de disociación[32].

Las necesidades de la propia persona o la confianza que ha depositado en otros le conducen a revelar aspectos íntimos o la situación en que se encuentra como es el caso de los testamentos ante notarios o el establecimiento de la tutela cautelar o autotutela[33]. Esta comunicación convierte a los

---

[30]Por su importancia es considerado un dato especialmente protegido, en el mismo apartado se considera la ideología, afiliación sindical, religión, creencias y el origen racial, por mencionar algunos.

[31]LDPPP. Art 3.-VI. Datos personales sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

[32]LDPPP. Art 3.-VIII. Disociación. El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo"

[33]LEY 41/2003, de 18 de noviembre, de protección patrimonial de las personas con

profesionales en confidentes privilegiados de una situación, Eesta confianza exige respeto y lealtad así como un conocimiento de los mecanismos de seguridad para preservar esa información privilegiada. El notario es un garante de la información personal, misma que cada vez más se encuentra contenida en medios informáticos. Por ello deberá instrumentar una política de gestión de los datos personales, tomando en consideración el marco jurídico que regula la materia.[34]

6.- HACIA LA NOTARÍA AUTOMATIZADA Y LA NOTARIA DIGITAL

De acuerdo con el Informe de la Informatización de la Función Notarial, en todas las oficinas notariales se utilizan computadoras para el ejercicio de la función notarial, como procesadores de texto y como sistemas para organizar el trabajo de la notaría; el sistema operativo más utilizado es "Windows"; la mayoría de los notarios utiliza programas específicos de uso notarial; el uso del e-mail es mínimo, es decir, su potencial aún no se ha explotado al máximo y la

discapacidad y de modificación del Código Civil, de la Ley de Enjuiciamiento Civil y de la Normativa Tributaria con esta finalidad.

[34]A partir del 2013 el IFAI tiene la propuesta de "Guía para implementar un sistema de gestión de seguridad de datos personales". http://inicio.ifai.org.mx/DocumentosdeInteres/GuíaimplementaciónSGSDP.pdf misma que puede ser de gran utilidad para auxiliar la gestión notarial de datos personales en términos de seguridad informática.

mayoría de los notarios no considera tener capacidad para dar asesoramiento en un negocio jurídico realizado vía telemática[35]; si bien es cierto dicho informe tiene más de una década es lamentable que aún existan un porcentaje considerable de notarios ajenos y resistentes a este tópico, por ello se debe promover la capacitación y actualización a través de los diversos Colegios, Consejos, Asociaciones o Uniones que integran los notarios.

Según William B. Kennari, Escribano Notario de Londres, y en lo que respecta al sistema anglosajón señala que los "cybernotarios" podrán ofrecer servicios profesionales relacionados con la certificación y autentificación de las transacciones internacionales vía computadora a través de registros que garanticen su consentimiento y demuestren su validez y, por lo tanto, su carácter como transacciones internacionales en cualquier jurisdicción. Estos especialistas garantizarán la autenticidad y credibilidad de las transacciones hechas vía computadora desde su misma existencia, incluyendo su creación, comunicación, procedimiento, retención y capacidad probatoria, porque una de las responsabilidades de estos especialistas será paralela con la de aquellos notarios que ejercen en los países del sistema latino o del "civil law", donde se ha establecido una profesión notarial muy sólida (Kennari, 1998).

[35]http://www.juridicas.unam.mx/publica/librev/rev/podium/cont/21/cnt/cnt3.pdf, consultado el 17 de marzo de 2009.

Por otro lado, aunque en México el tema de las Autoridades Certificadoras por medio del cual se define y reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y las firmas digitales no está resuelto completamente; la instrumentación de éstas es el camino por donde aparecerán nuevas funciones notariales, como sucede en España, en donde se encuentra previsto como una entidad que cumpliría esta función. Por esto, en el presente artículo se examinaron *grosso modo* los diferentes conceptos que son necesarios para la correcta compresión en la construcción de una Notaría Digital; además de un panorama acerca del funcionamiento de las mismas y del manejo de los certificados digitales.

Esta Notaría Digital valida identidades y proporciona certificados de servidor y cliente. Estos últimos representan una ventaja para el usuario ya que permiten, entre otras cosas, el intercambio seguro de correo electrónico, garantizando la integridad y confidencialidad del mismo. Es precisamente esto, lo que la convierte en una opción atractiva para el usuario, al permitirle depositar sus datos con confianza en la red.

Una de las mayores debilidades que tiene la información digital es su "volatilidad". Con la misma sencillez que puede ser tratada, procesada o transmitida, puede ser copiada, borrada y modificada de manera no autorizada. Sí se pretende que esos datos tengan validez y eficacia jurídica, se acaba recurriendo a métodos de notaría tradicional. Una

solución a estos problemas la constituyen los servicios de notaría digital, un servicio que permita probar en cualquier momento, de una manera irrefutable matemáticamente, que en determinada referencia temporal unos documentos en formato electrónico existían y que no han sido modificados desde entonces.

El modelo de notaría digital busca constituirse en alternativa a la notaría tradicional en medios electrónicos y en soporte fundamental para el surgimiento y generalización de nuevos servicios de comercio electrónico a través de Internet, pudiendo emplearse para la resolución de conflictos si se respetan las condiciones dispuestas por la legislación. Este servicio, además, pretende integrarse con las plataformas y escenarios habituales de un proveedor de servicios de Internet (ISP), ampliando su oferta de servicios al cliente, con soluciones tecnológicamente avanzadas (Higuero, Pérez, Muñoz, et. als. 2001). Esta salida resolverá muchos de los argumentos que se ha esgrimido de la lentitud de los trámites en los escenarios actuales de las notarías latinas de corte clásico.

En México el uso de certificados emitidos por la Red de Certificación Digital que tiene convención la Asociación Nacional del Notariado Mexicano A.C. y Acertia.com, es necesaria para dar seguridad y confiabilidad al uso de firmas electrónicas en comunidades amplias y a gran escala. Así se soluciona el problema de seguridad garantizando la integridad, autenticidad y el no rechazo de origen.

En México, con el conjunto de reformas legales aplicables a este tema se hace posible la firma electrónica, en sus dos niveles, proporcionando el sustento legal necesario para su funcionamiento. El medio del comercio telemático y estos avances dentro de la economía y el entorno virtual, constituyen un desafío para la supervivencia de nuestra profesión notarial de la manera tradicional (Pérez y Micolli, 1998).

CONCLUSIONES

1. El notario público como profesional del derecho en esta sociedad del conocimiento requiere adentrarse y tener los conocimientos fundamentales sobre seguridad informática para poder gestionar adecuadamente la información bajo su responsabilidad. Particularmente proteger los datos personales de los particulares a los que les presta el servicio, teniendo en cuenta los derechos de la protección de los datos personales y los de autodeterminación informativa.

2. La ofimática notarial es una vertiente de la informática jurídica que está iniciando su desarrollo en el campo de los programas adecuados para garantizar un buen servicio notarial. Esta nueva disciplina en desarrollo, establecerá las particularidades para la operación con calidad de las notarías automatizadas y aquéllas que presten servicios de instancias certificadoras.

3. La firma electrónica es un mecanismo informático que paulatinamente se ha incorporado a la función notarial como instrumento reconocido por la normatividad como un elemento de garantía y seguridad de las operaciones del comercio electrónico, así como mecanismo que se utiliza para gestionar información registral y catastral rápida para el desarrollo de las operaciones entre particulares así como para el cumplimiento de obligaciones fiscales.

4. La información de las personas depositada en los archivos electrónicos y bancos de datos del despacho notarial implican un responsabilidad ligada al deber de cumplir con el secreto profesional del notario, lo que supone que la gestión adecuada de esa información con estándares de seguridad, es tarea importante de las decisiones del titular del despacho para evitar responsabilidades de carácter jurídico, civil, administrativa o incluso penal.

5. Los despachos notariales se orientan a convertirse en notarías digitalizadas o notarías digitales, que no son exactamente lo mismo. Por un lado los despachos para el cumplimiento de sus funciones tradicionales incorporan equipo y programas adecuados y actualizados con la finalidad de aprovechar los avances tecnológicos tanto privados como públicos para acelerar sus procedimientos y métodos de trabajo y, por otro, se incorporan al medio virtual por medio de internet para cumplir la función de realizar funciones similares de fedatario pero en un entorno electrónico mediante la autorización de instancias de certificación

como es el caso de la firma electrónica y algunas otras intervenciones notariales.

6. Conforme se incorporan a la legislación mercantil, civil, administrativa y penal entre otras áreas, los conceptos relacionados con el derecho informático y la informática jurídica, también se hace necesario el estudio específico de la teoría jurídica de esta materia así como la jurisprudencia correspondiente. El derecho informático gradualmente se relaciona más con los otros ámbitos de las disciplinas jurídicas, lo que implica la relación inevitable entre éste y el derecho notarial.

REFERENCIAS

Alfín Martín-Gamero, José María. (2009). Aspectos técnicos y jurídicos de la firma electrónica. *Revista Informática Jurídica*. Extraído el 13 de marzo de 2009, de http://www.informatica-juridica.com/trabajos/aspectos_tecnicos.asp.

B. Kennari, William. (1998, julio-diciembre). El Concepto y el Desarrollo del Cibernotary. *Podium Notarial, Revista del Colegio de Notarios del Estado de Jalisco*, (18). Extraído el 17 de marzo de 2009, de http://www.juridicas.unam.mx/publica/librev/rev/podium/cont/18/cnt/cnt4.pdf

Bailón Cabrera, Lorenzo. (2005, diciembre). El derecho fundamental de la protección de derechos personales. *Podium Notarial, Revista del Colegio de Notarios del Estado de Jalisco*, (32). Extraído el 17 de marzo de 2009, de http://www.juridicas.

unam.mx/publica/librev/rev/podium/cont/32/pr/pr38.pdf

Beck, U. (1994). *La sociedad del riesgo. Hacia una nueva modernidad*. Barcelona. Paidós

Carreño, L. P., y Moreno, J. (2002). *Construcción de una notaría digital*. Colombia, Universidad de Bucaramanga.

Cornejo López, Valentino. (2001, abril). Una realidad mexicana, la firma electrónica y la participación del notario mexicano. *Revista de Derecho Informático*: Alfa-Redi , (33).

Durán Loera, Carlos Alejandro. (2007). Informática jurídica del derecho notarial y del derecho registral. *Revista de Derecho Notarial, Asociación Nacional del Notariado Mexicano, A.C.*, (121) (pp. 153-154).

Higuero Mariví, Pérez Igor, Muñoz Alejandro. *Sistema de Notaría Digital: certificación, sellado en el tiempo y validación de documentos digitales*. Grupo de Ingeniería Telemática. Departamento de Electrónica y Telecomunicaciones: Universidad del País Vasco.

Lozano, M. (1982). *Los grandes sistemas jurídicos.* Madrid. El Debate.

Lynch, H. (1996). *Notas sobre el derecho en la era digital*. La Ley. Extraído de http://works.bepress.com/horacio_m_lynch/25/.

Morales, F. (1984). *La tutela penal de la intimidad: privacy e informática*. España, Destino.

Pérez Fernández Del Castillo, Bernardo. (2000, mayo-agosto). Perfil del Notario en el Siglo XXI. *Podium Notarial, Revista del Colegio de Notarios del Estado de Jalisco*, (22). Extraído el 17 de marzo de 2009, de http://www.juridicas.unam.mx/publica/rev/indice.htm?r=podium&n=22.

Pérez Montero, Hugo y Micolli, Mario. (1998, julio-diciembre). Problemática actual de la contratación a distancia, *Podium Notarial, Revista del Colegio de Notarios del Estado de Jalisco*, (18). Extraído el 17 de marzo de 2009, de http://www.juridicas.unam.mx/publica/librev/rev/podium/cont/18/cnt/cnt6.pdf

Ramos Suárez, Fernando. (1999, abril). La Firma Digital. *REDI Revista Electrónica de Derecho Informático*.

Reusser, Calos Patricio. (2003). Qué es la sociedad de la información? *AR: Revista de Derecho Informático,* (61). Extraído de http://dialnet.unirioja.es/servlet/articulo?codigo=649933

Reyes, A. (2004). *Firma Electrónica*. México, Porrúa.

Ribagorda, A. (1996). *Seguridad informática. Ámbito jurídico de las tecnologías de la información*. Madrid. Consejo General del Poder Judicial, 309.

_____. (2000). *Seguridad informática. Derecho del comercio electrónico*. Madrid. La Ley.

Ríos, J. (1995). *La práctica del derecho notarial*. México, Mc Graw Hill.

Ríos, J.J. (1997). *Derecho e informática en México. Informática jurídica y derecho de la informática.* México. Instituto de Investigaciones Jurídicas.

Suprema Corte de Justicia de la Nación. (2006). *El juzgador y la informática jurídica.* [Compilación]. México: Dirección General de la Coordinación de Compilación y Sistematización de Tesis.

Téllez, J. (2003). *Derecho Informático.* México. Mc Graw Hill.

Trueba Buenfil, Fernando. (2007). El comercio electrónico, la firma digital, la certificación y el Notario. *Revista De Derecho Notarial, Asociación Nacional del Notariado Mexicano, A.C.,* (120) (p. 83).

Vidal Domínguez, Ignacio. (2002). El secreto profesional ante el notario. *Ius et Praxis versión on-line*, *8*, (2).

Villanueva, E., y Nucci, H. (2012). *Comentarios a la Ley Federal de Datos Personales en Posesión de Particulares.* México. Novum.

ANÁLISIS DE LA LEY QUE GARANTIZA LA TRANSPARENCIA Y EL DERECHO A LA INFORMACIÓN PÚBLICA PARA EL ESTADO DE CHIAPAS*

INTRODUCCIÓN

Las sociedades democráticas de esta Aldea Global, hacen más evidente que la información fue y es uno de los elementos que contribuye de manera sustantiva a la calidad de la comunicación para una adecuada convivencia social[1]. Por ello, la existencia y disposición de información veraz y precisa, permite a los ciudadanos tomar decisiones apropiadas para su participación en los diversos espacios sociales en que se desarrollan[2].

---

[1]La Suprema Corte de justicia de la Nación ha establecido sobre este derecho: "esa garantía se encuentra estrechamente vinculada con el respeto a la verdad. Tal derecho es... básico para el mejoramiento de una conciencia ciudadana que contribuirá a que esté mejor enterada, lo cual es esencial para el progreso de nuestra sociedad" Semanario Judicial de la Federación, novena época, tomo III, junio de 1996. Garantías individuales (derecho a la información), tesis P.LXXXIX/96, núm. de registro 200, 111, aislada. Suprema Corte de Justicia de la Nación, pleno, solicitud 3/96.

[2]El Derecho de acceso a la información en el marco jurídico interamericano = the inter-American legal framework regarding the right to access to information / Relatoría Especial para la Libertad de Expresión, Comisión Interamericana de Derechos Humanos- De otra parte, el libre acceso a la información es un medio para que, en un sistema democrático representativo y participativo, la ciudadanía pueda ejercer adecuadamente sus derechos político.

No obstante la importancia de ésta, desde siempre; los medios de acceso a la información pública de manera masiva y electrónica son relativamente de nueva aparición, lo que ha configurado hoy en día lo que se conoce como la era digital. Esta situación explica la existencia reciente, muy dinámica por cierto, de un marco legal adecuado que garantice el acceso a la información y su uso correcto[3], además de obligar a los gobiernos a aplicar políticas públicas para informar y transparentar el uso de los recursos y los temas de interés público como una acción democrática.

Estamos ubicados en la coyuntura de la Sociedad de la Información y de los derechos emergentes[4] vinculados a ella. La aceptación generalizada de dicho concepto, responde a la cantidad y gran movilidad de la información existente; en virtud de su manejo y explotación por los medios de comunicación. Este concepto surge de forma contemporánea al desarrollo de la sociedad capitalista, que requiere de un mercado global, en la que las características de la organización social conceden un lugar privilegiado y determinan-

[3]Eduardo Flores-Trejo, Derecho de acceso a la información: de la fase normativa a la valoración de su impacto. Publicado en la Revista del CLAD Reforma y Democracia. No. 35. (Jun. 2006). Caracas. "Lo realmente sorprendente es que, a pesar de que el derecho a la información, en su sentido amplio, fue reconocido desde 1948 en la Declaración Universal de los Derechos Humanos de la Organización de las Naciones Unidas (artículo 19), más de la mitad de esas leyes han sido promulgadas apenas en los últimos 10 años".

[4]Perrine Canavaggi. El acceso a la información pública en el mundo un derecho humano emergente. 7º Seminario Internacional de Archivos de Tradición Ibérica. Rio de Janeiro. 27 de Junio a 1 de Julio de 2011.

te desde el punto de vista económico, al papel que juegan las tecnologías relacionadas con la información; e incluso la misma es considerada como mercancía de estratégica importancia y gran valor. Por ello se hace necesario el desarrollo de su tutela jurídica[5].

En esta Sociedad de la Información y el Conocimiento[6] como finalmente es clasificada por diversos académicos[7], han surgido nuevas expresiones acerca de los derechos fundamentales o al menos los ha hechos más evidentes y necesarios[8]. Uno de ellos, que ha tenido una dinámica re-

---

[5]Téllez Valdez Julio. Derecho informático versión electrónica. Pág. 45. http://biblio.juridicas.unam.mx/libros/1/313/5.pdf.

[6]Carlos Patricio Reusser. ¿Qué es la sociedad de la información? En los últimos quince años, y especialmente en la década de los noventa, ha cobrado auge y difusión nacional y mundial el concepto de "Sociedad de la Información" (SI), sobre todo por su gran promoción en el ámbito de las políticas públicas, utilizándose de mejor o de peor manera para referirse, en general, a cualquier cuestión derivada de innovaciones tecnológicas que han devenido en un cambio en el modelo social.

[7]Sociedad de la información o sociedad de la comunicación son expresiones utilizadas en las ciencias sociales para calificar a las sociedades industriales y postindustriales contemporáneas en su fuerte dependencia de los medios de comunicación de masas y, más recientemente aún, de las tecnologías de la información y comunicación y las redes sociales. http://es.wikipedia.org/wiki/Sociedad_de_la_informaci%C3%B3n

[8]El derecho a la información, en términos de Sergio López-Ayllón, no es sino la reformulación jurídica de las libertades tradicionales de expresión e imprenta para adaptarlas a las nuevas condiciones de la información a finales del siglo XX. El derecho a la información (contenido en la libertad de expresión en sentido amplio) es la garantía que tienen las personas de conocer de manera activa –es decir, investigando – o pasiva – recibiendo – las ideas, opiniones, hechos o datos que se producen en la sociedad y que les permiten formarse su opinión dentro de la pluralidad, diversidad y tolerancia que supone una sociedad democrática.

levante, es el derecho de acceso a la información pública[9]. La Corte Interamericana de Derechos Humanos, en el caso Claude Reyes y otros, marcó un precedente jurisprudencial al ser el primer tribunal internacional en reconocer que el acceso a la información es un derecho humano implícito en el derecho a la libertad de expresión. Previamente, la Comisión Interamericana de Derechos Humanos y la Relatoría Especial para la Libertad de Expresión venían impulsando avances en la materia a través de sus diferentes mecanismos de trabajo.

El antecedente histórico más remoto se registra en Suecia, con la publicación de la Ley de Libertad de Prensa de 1776, en la que se hace el reconocimiento jurídico del derecho de acceso a la información . A partir de ello, se pueden distinguir cuatro olas de legislaciones; la primera es la de los diez países pioneros: después de Suecia (1766) y Finlandia (1951), los Estados Unidos adoptaron el Freedom of Information Act (FOIA) en 1966, seguidos por Dinamarca y Noruega (1970), Francia y Países Bajos (1978), Australia y Nueva Zelandia (1982) y por último Canadá (1983); la

[9]Miguel Carbonell. El derecho de acceso a la información como derecho fundamental. Instituto de investigaciones jurídicas del UNAM. A la luz de lo anterior podríamos preguntarnos, ¿es necesario que la transparencia y el derecho de acceso a la información sean un derecho fundamental? Si revisamos su contenido posible podremos convenir en que el derecho de acceso a la información tiene por objeto la protección de bienes básicos. Dicha protección opera de dos distintas maneras: a) la primera es en relación a la posibilidad de darle contenido, calidad y sustancia a otros derechos fundamentales, y b) la segunda reside en el valor autónomo que tiene la información como bien jurídico.

segunda ola es la de los países que, después del derrumbamiento de los regímenes autoritarios, adoptaron una ley durante los años 1990-2000, con motivo del establecimiento o restablecimiento de las instituciones democráticas; la tercera es la de los 13 países ricos y de tradición democrática que lo hicieron en el marco de la reforma y modernización administrativa.

Desde hace unos diez años, asistimos a una auténtica explosión mundial de las leyes sobre el acceso a la información, incluso en países en desarrollo que no han tenido transición democrática. Trece países tenían una ley de este tipo en 1990, y son 87 en 2011 los que la han adoptado. Latinoamérica es un buen ejemplo, ya que en diez años once países del área han votado un ordenamiento de esta naturaleza: Panamá (2002), Perú (2002), México (2002), la República Dominicana (2004), Ecuador (2004), Honduras (2006), Nicaragua (2007), Guatemala (2008), Uruguay (2008), Chile (2008), y más recientemente, El Salvador, en Marzo de 2011".[10]

A partir de 1990, la democratización en el mundo se vio acompañada por un desarrollo sin precedentes de leyes de acceso a la información. No obstante eso, es hasta el segundo semestre del 2005 que en 62 países ya se habían adoptado legislaciones para la protección del derecho de acceso a

[10]Perrine Canavaggi. El acceso a la información pública en el mundo un derecho humano emergente. 7º Seminario Internacional de Archivos de Tradición Ibérica. Rio de Janeiro. 27 de Junio a 1 de Julio de 2011.

la información en un periodo relativamente reciente[11]. En la actualidad existen más de 95 ordenamientos en la materia a nivel internacional, más de una decena de estas leyes fueron generadas en países de América Latina[12].

Como consecuencia de este proceso, nuestro país se ha inscrito en esa tendencia, y en un periodo relativamente breve, la legislación federal y la de las entidades federativas incorporaron el marco jurídico para regular y protegerlo de diversa forma. En tal virtud y contexto, este análisis se orienta principalmente a revisar el tema de la legislación que regula este derecho fundamental[13] en el Estado de Chia-

[11]Verificar en el Séptimo cuaderno de Transparencia del IFAI, presentación de John M. Ackerman e Irma E. Sandoval. Cuento clásico sobre la "Ley Para la libertad de Prensa y del derecho de acceso a las actas públicas". LA PRIMERA LEY FORMAL DE ACCESO A LA INFORMACIÓN FUE LA FREEDOM-OF- PRESS AND THE RIGHT-OF-ACCESS TO PUBLIC RECORDS ACT (Ley para la Libertad de Prensa y del Derecho de Acceso a las Actas Públicas) aprobada en Suecia en 1766, diez años antes de la Independencia de los Estados Unidos y trece antes de la Revolución Francesa. El principal impulsor de esta ley fue el sacerdote y diputado Anders Chydenius, quien a su vez se inspiró por las prácticas contemporáneas en China. De acuerdo a Chydenius, China fue "el país modelo para la libertad de prensa" y el ejemplo a seguir por otras naciones en esa materia.

[12]Al menos 95 países alrededor del mundo han adoptado leyes de acceso a la información. Este mapa de Social Science Research Network muestra los esfuerzos de esas naciones y las que tienen medidas pendientes. En América Latina casi todas las regiones tienen normas adecuadas o las están preparando. Hay dos excepciones: Venezuela y Guyana.

[13]No debemos confundir el concepto más amplio de derecho a la información con el derecho de acceso a la información pública tan en boga últimamente, ya que éste último es un derecho subsidiario del derecho a la información en sentido amplio y podría definirse como la prerrogativa que tienen los ciudadanos para acceder a datos, registros y todo tipo de informaciones en poder de entidades públicas y empresas privadas que ejercen gasto público y /o cumplen funciones de autoridad, con las excepciones que les marque la ley.

pas, para estudiar el grado de tutela que alcanza hasta ahora, qué características tiene y el impacto regulatorio que ha alcanzado hasta ahora.

ANTECEDENTES

En el ámbito concreto del derecho a la información, debemos recordar que en 1948[14] es reconocido como un derecho humano fundamental[15]; entendido como la facultad que tienen las personas para atraerse información, informarse y ser informadas.

Respecto a su fundamento constitucional en México, fue en el marco de la reforma política del estado durante 1976, que se adicionó al artículo 6º de nuestra Carta Magna, el párrafo que señala: "el derecho a la información será

---

[14]Jorge Carpizo / Ernesto Villanueva. Derecho a la información en México: propuestas para su regulación. En 1948 con la Declaración Universal de los Derechos del Hombre nace realmente la garantía fundamental del derecho a la información, aunque existían antecedentes; éste es el resultado de una hermosa evolución histórica y jurídica. El derecho a la información, de acuerdo con el Artículo 19 de esa Declaración Universal, es la garantía fundamental que toda persona posee para atraerse información, informar y ser informada.

[15]El derecho de acceso a la información es esencial para la consolidación, el funcionamiento y la preservación de los sistemas democráticos. En este sentido, la jurisprudencia de la Corte Interamericana de Derechos Humanos ha señalado que el actuar del Estado debe encontrarse regido por los principios de publicidad y transparencia en la gestión pública, lo que hace posible que las personas que se encuentran bajo su jurisdicción ejerzan el control democrático de las gestiones estatales, de forma tal que puedan cuestionar, indagar y considerar si se está dando un adecuado cumplimiento de las funciones públicas

garantizado por el Estado". En ese entonces, esta reforma se encaminó principalmente a los partidos políticos, con la finalidad de que tuvieran acceso pleno a los medios de información, para difundir su ideología; y no para que los ciudadanos pudieran acceder a la información del estado.

No obstante, lo dispuesto en este precepto constitucional que fue el punto de partida, es hasta el año 2002, cuando se creó el marco jurídico federal para garantizar el acceso de los ciudadanos a los documentos, archivos y datos del gobierno federal y es a partir de junio de 2003 cuando la Ley Federal de Transparencia y Acceso a la Información Pública entra en vigor, regulando el tema de transparencia y derecho de acceso a la información pública, así como lo relativo al derecho humano a la protección de datos personales en posesión de la administración pública, y establece la existencia de una organismo que garantiza este derecho; el IFAI (órgano garante del ejecutivo federal) además determina las causas de responsabilidad, aunque el Órgano de Control Interno de cada Poder es quien finca responsabilidades.

Para tener una idea del avance, los últimos datos que proporciona la institución sobre el uso de visitas al Portal de Obligaciones de Transparencia (POT) de las dependencias y entidades de la Administración Pública Federal ha sido de más de 100 millones de 2007 a diciembre de 2013. Para tener otra idea acerca del conocimiento de este derecho en la instancia nacional, durante el 2013 existen registros de que, el Pleno resolvió un total de 7 mil 506 recursos de revisión,

interpuestos por particulares que se inconformaron por las respuestas negativas que recibieron a sus solicitudes de información hechas a dependencias y entidades de la APF[16]. Esto significa que un importante número de los ciudadanos mexicanos, han hecho efectivo su derecho de acceso a la información pública.

En lo que respecta a las entidades federativas, Jalisco fue el primer estado de la República Mexicana en promulgar una ley tipo en la materia durante diciembre del 2001; actualmente todos los estados cuentan con un ordenamiento similar. Cabe hacer mención, quede entre las leyes estatales, los expertos han comentado como realmente avanzadas en su diseño legislativo a las de Sinaloa, Morelos, Michoacán, Durango y Yucatán; esto porque cumplen en su mayoría con los principios básicos del Derecho a la información[17].

Las leyes locales más cuestionadas por ser contrarias a los principios rectores son las de Jalisco y Nuevo León, ya que se las acusa de obstaculizar el acceso a la Información y no definir de manera adecuada y en beneficio de la ciudadanía los casos de reserva de la información. El periodo de vigencia que tienen las leyes estatales ha sido evaluado y

[16]Datos tomados del portal del IFAI. http://inicio.ifai.org.mx/_catalogs/masterpage/ifai.aspx

[17]Tener una adecuada legislación no implica que su implementación sea esta eficiente, por ello se han hecho diversos estudios aplicando diversas metodologías para evaluar el avance de la observancia de este derecho fundamental en los estados de la república.

clasificado; no obstante el marco jurídico integral desprendido de ellas, el reenvío o relación en la interpretación y aplicación de la ley de acceso, la reglamentación administrativa y el desarrollo de portales para poner la información a disposición está pendiente

La primera generación de leyes locales en la materia se da en el año 2002 cuando todas las entidades federativas del país habían publicado leyes de transparencia. La práctica del derecho de acceso a la información hizo notoria una serie de fallas provocadas por la heterogeneidad de las leyes: requisitos que volvían nugatorio el derecho de los ciudadanos a obtener información pública; obligación de estampar firma autógrafa en la solicitud, como lo fue en el caso de nuestra entidad federativa; un mal diseño del medio de impugnación, tal como sucede con el recurso de revisión y que aquí se llamó reconsideración; la acreditación de personalidad del solicitante (identificación) se establecía como obligatoria y no contemplaba la posibilidad de presentar solicitudes vía electrónica. La orientación era hacia una importante cantidad de causales de reserva que convertían a las leyes de transparencia en leyes de "máxima reserva", sin especificar sanciones precisas en caso de incumplimiento.

En la primera generación de leyes estatales, no en todos los casos, no existía un organismo garante ante el cual pudieran acudir los ciudadanos, o bien, no contaban con las facultades suficientes para hacer efectivo este derecho. En muchos casos, la resolución de inconformidades (recurso de

revisión) era competencia de otras instancias, mayormente del poder judicial.

La reforma del 2007 al artículo 6° Constitucional, surgió desde lo local por la propuesta de los Gobernadores de Aguascalientes, Chihuahua y Zacatecas, a la que se sumaron el Distrito Federal y Veracruz, junto con la Conferencia Mexicana de Acceso a la Información Pública (COMAIP). Fue así como presentaron la iniciativa al H. Congreso de la Unión, tomando como punto de partida, la famosa Declaración de Guadalajara.

Con esta reforma, los principios para garantizar el DAI se contemplaron por primera vez, éstos fueron consagrados en el artículo 6º de la Constitución Política de los Estados Unidos Mexicanos, que al efecto establece:

> Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:
>
> Toda la información es pública, la información podrá ser reservada sólo en los términos que marcan las leyes, deberá prevalecer el principio de máxima publicidad. Protección de la vida privada y los datos personales, no acreditación de interés jurídico, Derechos ARCO. Mecanismos de acceso a la información y procedimientos de revisión expeditos ante órganos u organismos especializados e imparciales, y con autonomía operativa, de gestión y de decisión. Obligación de preservar sus documentos en archivos y de publicar indicadores de gestión. Publicar información relativa a los

> recursos públicos que entreguen a personas físicas o morales. Sanciones en caso de incumplimiento. Se aplica una política pública nacional con la finalidad de lograr que las características que deben tener las Leyes de Acceso de las entidades federativas observe los menores límites posibles al Derecho de Acceso a la Información Pública (causales de reserva), que contengan las Definiciones y conceptos que precisen los Sujetos Obligados que le den un lugar preponderante a la Promoción de la Cultura de Apertura de Acceso a la Información de Oficio, que se aplique el principio esencial de la Máxima Publicidad que se incorpore la Interpretación de la Gratuidad y que la naturaleza jurídica del Órgano Garante Autónomo y que los criterios de Clasificación de la Información Protección de datos personales, que se establezcan Procedimientos Recursos adecuados y que las Sanciones Administrativas y que se considere el Principio de Definitivita de las resoluciones.

Por su parte, la Constitución reformada de Chiapas[18], en su artículo 3º correspondiente a los derechos humanos, contempla ahora lo relacionado con nuestro tema en la fracción XIX, estableciendo que "toda persona tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas,

[18]Última reforma: Decreto 028, publicado en el Periódico Oficial 399, de fecha miércoles trece de Noviembre de 2012, Anexo página 107. Esto como parte de la inclusión de los 30 artículos de la Declaración Universal de los Derechos Humanos y los Objetivos de Desarrollo del Milenio (ODM) de la ONU, en la reforma constitucional que se le dio por llamar la constitución siglo xxi. Que incorporó una parte dogmática en un cuerpo normativo local que principalmente regulan aspectos orgánicos.

sin limitación de fronteras, por cualquier medio de expresión"; lo que implica el reconocimiento constitucional local al derecho a la información. Con ello ratifica el contenido previsto en la Constitución de los Estados Unidos Mexicanos, en los artículos 6º, 7º y 8º, y plantea como parte de las garantías individuales el derecho a la información.

Como ya apuntamos en abril de 2002, se promulgó la Ley Federal de Transparencia y para finales del año 2006, todas las entidades federativas del país contaban con su respectiva legislación en la materia, incluso alguna de ellas más avanzada que la nacional, como fue el caso de Sinaloa[19]. En Chiapas este proceso llegó tarde, para no perder la tradición de los cambios históricos extemporáneos, la Ley que Garantiza la Transparencia y el Derecho a la Información Pública para el Estado de Chiapas, fue expedida mediante Decreto número 412 de fecha 11 de octubre de 2006, siendo publicada en el Periódico Oficial del Estado número 388 del 12 de octubre del mismo año, sólo los estados de Hidalgo y Tabasco le sucedieron[20].

En este contexto el periodista Isaín Mandujano, quien apoyó desde LIMAC el avance de la materia en la

[19]Kate Doyle. Cometarios a Ley Federal de transparencia y de acceso a la información pública. http://www.juridicas.unam.mx/publica/rev/decoin/cont/2/cmt/cmt7.htm

[20]Isaín Mandujano en su página web apuntaba "La nueva Ley de Acceso A la Información y Transparencia del Estado de Chiapas, siendo una de las últimas legislaciones en materia de transparencia ocupa el lugar veintinueve de las treinta legislaciones en el país", dijo Perla Gómez Gallardo en octubre pasado.

entidad, en su tiempo señaló respecto de la primera ley de Chiapas:

> La nueva Ley de Acceso a la Información y Transparencia del Estado de Chiapas, siendo una de las últimas legislaciones en materia de transparencia ocupa el lugar veintinueve de las treinta legislaciones en el país
>
> "Y cierto, haciendo un somero análisis de artículo por artículo se puede deducir que esa ley, está más hecha a la medida para inhibir el acceso a la información pública y aparentar la transparencia que realmente para dar cabal cumplimiento a ese derecho ciudadano

Además apuntaba:

> sin embargo, si bien éste articulado es coherente con los lineamientos básicos de toda ley sobre la materia, esta se contradice con el artículo 16 de la misma ley, pues en uno de sus apartados donde se exige "nombre completo del solicitante y documento oficial de identificación", además se pide que la solicitud debe contener "firma del solicitante o su representante. En caso de que no pueda o no sepa escribir el solicitante imprimirá su huella digital.[21]

En sus conclusiones, afirmó, en aquel momento:

> En síntesis, esta ley es un instrumento jurídico sin coherencia y secuencia lógica, por ello es menester tener cuidado

[21]Isaín Mandujano. LA LEY TRANSPARENCIA DE CHIAPAS, CONTRADICCIONES Y RETROCESOS Las trampas de la ley, artículo por artículo enero 17, 2007. http://isain-mandujano.blogspot.mx/2007/01/la-ley-transparencia-de-chiapas.html

> al momento de hacer uso de ella. Antes es necesario hacer un análisis, interpretarla, tratar de encontrar sus fortalezas y debilidades. Aprovechar pues las pocas o muchas ventajas que pueda ofrecer. Es una ley que no está sistematizada. Parece más bien un rompe cabezas donde todas las piezas están dispersas y algunas más no se encuentran en la mesa.

Cabe destacar que con las reformas aprobadas al artículo 6º Constitucional, se establecieron criterios mínimos o los denominados "principios rectores[22] en materia de transparencia y de acceso a la información pública", lo que llevó a mejorar sustantivamente las leyes de transparencia de todos los estados del país; ahora sí, Chiapas fue la primera entidad federativa[23] en dar cumplimiento a este mandato constitu-

---

[22]Larenz, Karl: Metodología de la Ciencia del Derecho; IIª. ed., Ed. Ariel, S.A., Barcelona-Caracas-México, 1980, p. 465.Acerca de los principios generales del derecho se ha dicho que nacen como "principios ético-jurídicos" como criterios teleológico-objetivos de interpretación y en conexión con el desarrollo del Derecho atendiendo a un tal principio. Han sido considerados "pautas directivas de normación jurídica que, en virtud de su propia fuerza de convicción, pueden justificar resoluciones jurídicas". Han sido entendidos como "ideas jurídicas materiales" son acuñaciones especiales de la idea del Derecho, tal como ésta se presenta en su grado de evolución histórica. Algunos de ellos están expresamente contemplados en la Constitución u otras leyes; otros pueden ser deducidos de la regulación legal, de su conexión de sentido, por la vía de la "analogía general" o del retorno a la ratio legis; algunos han sido "descubiertos" y declarados por primera vez por la doctrina o por la jurisprudencia de los tribunales, las más de las veces atendiendo a casos determinados, no solucionables de otro modo, y luego se han impuesto en la "conciencia jurídica general" gracias a la fuerza de convicción a ellos inherente.

[23]En la exposición de motivos de la iniciativa se dijo: En tal virtud, y para estar en congruencia al Decreto de la Comisión Permanente del H. Congreso de la Unión, respecto a la adición del segundo párrafo y las siete fracciones al artículo sexto de la Constitución Política de los Estados Unidos Mexicanos, publicada en el Diario Oficial de la Federación de 20 de julio del 2007, el Ejecutivo a mi cargo, atendiendo al mandato constitucional, y ante la necesidad de realizar las

cional, al aprobar mediante Decreto número 270, reformas y adiciones; así como laderogación de diversas disposiciones a la Ley de Transparencia, siendo publicadas en el Periódico Oficial del Estado número 043, de fecha 29 de agosto de 2007.

LA LEY DE CHIAPAS Y SU EVOLUCIÓN LEGAL

A partir del 01 de enero de 2008, la Ley que Garantiza la Transparencia y el Derecho a la Información Pública para el Estado de Chiapas obliga a todas las Dependencias, Entidades y Órganos Desconcentrados de Gobierno del Estado, de los Gobiernos Municipales a facilitar el acceso a la información contenida en sus documentos, manejo de recursos públicos, resultados y desempeño.

Esta ley ha tenido otras reformas que están relacionadas con el Periódico Oficial No. 110, de fecha 13 de agosto de 2008; Periódico Oficial No. 123, de fecha 29 de octubre de 2008; Periódico Oficial No. 267, de fecha17 de noviembre de 2010, y la última del Periódico Oficial No. 336, de fecha 16 de noviembre de 2011.

La primera modificación a esta ley fue la del 29 de agosto de 2007, en la que los artículos 3º, 13, 15, 17, 21, 22, 38 y 66

---

modificaciones necesarias al marco jurídico en la materia estatal, establece en la presente iniciativa las adecuaciones jurídicas para el respeto y cumplimiento por parte de las autoridades estatales al derecho subjetivo público de dar a conocer la información pública de oficio a los gobernados, y con esto la rendición de cuentas para que prevalezca el estado de derecho democrático en nuestra entidad.

por mencionar algunos, sufrieron cambios. Con esta reforma, se abordó el acceso a la información pública, así como el procedimiento para acceder a ella; algunas definiciones, por ejemplo el concepto de documento e información reservada se establecieron; asimismo, se determinó la posibilidad de firmar convenios e intercambiar experiencias entre los sujetos obligados, el Instituto y las Unidades de Acceso, y se reformó lo referente a la forma en que deben ser presentadas las solicitudes de información, esto es en español y de forma educada, estando los sujetos obligados a dar contestación a toda petición.

Del mismo modo se reformó lo relacionado al inicio del procedimiento para solicitar información (artículo 17); además se precisó el término en el que la autoridad deberá comunicar al interesado la incapacidad de otorgarle información, cuando ésta sea catalogada como clasificada, fijando un plazo no mayor a 20 días (artículo 21); también lo relativo a la posibilidad de interponer el recurso consagrado en la ley sufrió cambio (artículo 22); se determinó que los sujetos obligados deberán preservar la información y documentación, así como a actualizarla cuando sea necesario (artículo 38) y lo relativo al órgano de vigilancia del Instituto también se transformó (artículo 66); por último, puede señalarse que se reformó el Título Tercero de la ley, relativo a la interposición del recurso de revisión, mismo que posteriormente sería derogado. Esta reforma, estableció la obligación de los sujetos a modificar o expedir nuevos reglamentos y adecuarlos a la nueva ley; se abrogo el Reglamento

Interior del Instituto, facultándolo a emitir otro dentro de un plazo no mayor a los 90 días.

Para el año 2008 (13 de agosto), se hicieron nuevas modificaciones a la Ley, de las que se exponen las siguientes: se reformó la fracción XX al artículo 37 relativa a qué información puede ser proporcionada por medios electrónicos; asimismo, se establecieron directrices para entender y aplicar lo consagrado en el artículo 70; la del 17 de noviembre de 2010, relacionada con la adición de una fracción al artículo que habla de la procedencia de la reserva de información (artículo 28 fracción XIII), ésta señala que será reservada la información que se encuentra clasificada por disposición expresa de otra ley, como de acceso prohibido o restringido.

La reforma más significativa que se ha realizado a la ley en estudio fue la del 16 del mes de noviembre del 2011, ya que fue en ésta que se derogaron diversas disposiciones así como se reformaron otras tantas, lo que hasta hoy es el derecho vigente y aplicable en esta materia. Dentro de las cosas que se pueden señalar de esta reforma es que se modificaron diversas disposiciones relativas al Título Primero de la Ley, tales como el artículo 1 que señala a los sujetos obligados el deber de considerar la información personal como privada, es decir, que por ninguna razón podrán hacerla pública ya que se encuentra clasificada como de acceso prohibido o restringido, estableciendo que la única forma en que se haga pública es a través del consentimiento del titular de la información.

De igual forma se modificó lo que debe entenderse por derecho de acceso a la información pública, información pública, datos personales, portal de transparencia, medios electrónicos y la adición de la prueba de daño. Se reestructuraron los principios que deben regir al acceso a la información pública, sus Unidades de Acceso , los requisitos para solicitarla, y se determinó el plazo de 20 días para dar contestación a las solicitudes de información; asimimso se reformó el capítulo II relativo a la reserva de información pública, y el III que habla de la información confidencial, ambos del Título Primero.

En lo concerniente a la protección de datos personales, se impusieron diversas cargas a los sujetos obligados, indicando que con el objeto de evitar la alteración, transmisión, pérdida o acceso no autorizado a los datos personales, deberían adoptar los mecanismos necesarios para su protección y tratamiento, garantizando la seguridad de los mismos.

Tal como se mencionó anteriormente, el recurso de revisión contenido en el Título Tercero, Capítulo II fue derogado, por lo que se tuvieron que hacer las modificaciones a las demás disposiciones jurídicas que emanaban de la ley en estudio.

También se hicieron cambios relacionados con Instituto de Acceso a la Información Pública, señalándolo como un organismo público descentralizado no sectorizable de la administración pública estatal, con personalidad jurídica y patrimonio propio, autonomía de gestión, así como, facultades de operación, decisión, resolución, administración, fomento, promoción y sanción en lo concerniente al dere-

cho de acceso a la información pública; se reestructuró su integración, pasando de tres a cinco consejeros, uno de los cuales tiene el carácter de Consejero General, llevando la representación legal del Instituto. En este sentido, también hubo cambios en la parte de los requisitos para ser consejero, así como de las atribuciones que tiene la propia institución, concediéndole la facultad de interpretar la Ley.

El Título Sexto, Capítulo I también fue objeto de reforma. Dicho capítulo habla del procedimiento de acceso a la información pública, indicando que toda persona tiene derecho a solicitar y recibir información, siempre y cuando siga el procedimiento establecido para tal caso y que exista una solicitud, misma que deberá ser de forma educada, clara y a través de los medios previamente establecidos para el fin.

Del mismo modo, se hicieron algunas modificaciones a apartado relativo a los recursos, los cuales deberán ser presentados ante el Instituto en donde los solicitantes que se consideren afectados por los actos y resoluciones del Comité o las Unidades de Enlace, por negar, limitar u omitir el acceso a la información pública, podrán promover el recurso de revisión ante la Unidad de Acceso a la Información Pública por escrito o a través de los medios electrónicos que pongan a disposición los sujetos obligados, señalando que la substanciación del mismo debe regirse por lo dispuesto en la Ley de Procedimientos Administrativos para el Estado de Chiapas, derogándose los demás artículos de este capítulo, salvo lo relativo al término en que la autoridad deberá contestar el recurso.

Por último, se reformó lo conducente a los costos de reproducción y envío, señalando que la información pública será entregada o enviada, una vez cubierto el costo correspondiente, cuando este proceda.

Por lo que de igual forma se modificó el Reglamento Interno del Instituto para adecuarlo, siendo estas cuatro reformas las que han cambiado el sentido original de la Ley.

Teniendo el contexto de los antecedentes de la evolución del derecho de acceso en el mundo y el país, este estudio hará una revisión a la forma de regular los principios rectores del derecho de acceso a la información que se derivan de la reforma constitucional y diversas interpretaciones a esos principios en múltiples casos, retomando los avances que diversas legislaciones locales, en particular la del Estado de Chiapas, han implementado para marcar un ejercicio comparativo con nuestro marco jurídico vigente en la entidad.

ESTRUCTURA Y CARACTERÍSTICAS

La Ley de Chiapas adolece en su denominación y estructura; ya que en primer término aborda el tema de la obligación del poder público de hacer transparente la gestión pública, y desde luego, es importante y relevante hacerlo, pero una ley que parte del reconocimiento del derecho pudo haber iniciado con una denominación en los siguientes términos, Ley de Derecho de Acceso a la Información Pública, Protección de Datos Per-

sonales y Transparencia de la Gestión Pública; y en ese orden estructurar los títulos, capítulos y secciones de la ley.

Así tenemos que el objeto y naturaleza jurídica de la ley, definido en su artículo primero, garantiza la trasparencia y en segundo y tercer término ubica la protección del derecho de acceso y la protección de los datos personales. En el caso de la legislación federal con mejor técnica legislativa establece como finalidad la garantía del acceso, y de igual manera lo hace el artículo primero de la ley de Sinaloa[24]. Hay precisar que la ley de Chiapas lo reconoce expresamente como un derecho fundamental como lo hace la ley del Distrito Federal por ejemplo.

Por lo que se refiere a los sujetos obligados la legislación de nuestro Estado, incluye a los tres poderes y órganos autónomos, no así a los partidos políticos, las empresas paraestatales, paramunicipales y cualquier instancia que maneje recursos públicos del estado y de los municipios, como por ejemplo sucede en el caso de la ley del Distrito Federal[25].

---

[24]La presente Ley es reglamentaria del artículo 109 Bis B de la Constitución Política del Estado de Sinaloa y tiene por objeto fijar los términos en que se garantiza y ejerce el derecho de acceso a la información pública como el correlativo al acceso y protección de datos personales, los que sólo serán limitados en los casos previstos expresamente por la Constitución como por esta Ley. (Ref. según Dec. No. 141 del 18 de julio del 2008, y publicado en el P. O. No. 100 del 20 de agosto del 2008.

[25]Mariana Cendejas Jáuregui. Breve análisis de la nueva Ley de Transparencia y Acceso a la Información Pública del Distrito Federal. "Por otro lado, se establece que toda persona moral, señalando a organizaciones de la sociedad civil, sindicatos o cualquier otra análoga que reciban recursos públicos por cualquier concepto, a excepción de las cuotas sindicales, debe proporcionar a los entes públicos de los que reciban recursos, la información relativa al uso, destino y actividades que realicen con éstos".

Respecto del artículo 3º, que contiene las definiciones de los conceptos que se utilizan en el texto legal, se encuentra completo y de manera semejante a los mejores ordenamientos de la materia.

Con relación al medio de impugnación, el artículo 22 de la ley local nos establece la posibilidad de que si el solicitante considera que su petición no fue satisfecha de la forma correcta, le da la posibilidad de interponer ante el órgano garante del acceso a la información, el recurso que contempla la misma ley en su Título Sexto, Capitulo II.

Este recurso es procedente cuando el solicitante considera afectado su derecho por el sujeto obligado, al negar, limitar u omitir el acceso a la información pública; asimismo, la propia legislación local contempla que podrá promover el recurso de revisión ante la Unidad de Acceso a la Información Pública por escrito o a través de los medios electrónicos que pongan a disposición los sujetos obligados.

El recurso contemplado en la ley local es muy distinto a lo que observan muchos cuerpos normativos en las demás entidades federativas; la coincidencia se da en los casos de procedencia del medio de impugnación, ya que cuando el sujeto obligado niega, limita y omite el acceso a la información a los particulares, se considera procedente, pero el mecanismo mediante el cual se tramita y resuelve es muy distinto.

Ahora bien, nuestra legislación contempla que para la sustanciación de este recurso de revisión, el órgano garante debe ajustarse a lo estipulado en el Libro Primero, Título

Séptimo, de la Ley de Procedimientos Administrativos para el Estado de Chiapas, asemejándose al procedimiento administrativo, debiendo seguirse y desarrollarse en dichos términos. Hay que hacer mención que este recurso se promueve ante un órgano diferente al que ocupa el sujeto obligado, mientras que en legislaciones como la de Aguascalientes, dicho recurso puede promoverse ante la propia autoridad que emite la resolución impugnada.

De igual modo, en otras entidades federativas como Colima, se contempla además la posibilidad de interponer un recurso de queja, siendo procedente cuando el sujeto obligado no dé contestación a la solicitud en el tiempo establecido y cuando se realicen investigaciones en relación a quejas sobre el incumplimiento de la Ley. Este recuso es procedente ante un órgano distinto al que se le solicita la información.

Ahora bien, existen otras leyes estatales que contemplan el recurso de reconsideración, tal es el caso de Morelos, donde se faculta al particular o solicitante para requerir a la autoridad nuevamente, a efecto de que emita un criterio respecto de una resolución pronunciada con anterioridad.

También, en la legislación del estado de Durango se considera la posibilidad de llegar a un acuerdo conciliatorio entre el particular o solicitante y el sujeto obligado, éste se presenta como un mecanismo antes de resolver el recurso de revisión; el proceso conciliatorio como lo señalé inicialmente se promueve antes de resolver la revisión, si no se llega a un arreglo conciliatorio se continua con el proce-

dimiento de revisión. Este mecanismo resulta muy interesante, ya que contribuye a resolver de forma más rápida las controversias que se susciten en este rubro, por lo que la legislación del estado de Chiapas debería considerar la posibilidad de incorporar dicha variante al recurso de revisión.

Respecto a los requisitos que debe satisfacer la solicitud, en el caso de Chiapas, se establecen en el Artículo 15:

> es obligación de los sujetos obligados recibir y dar trámite a todas las solicitudes de acceso a la información pública que les presenten, excepto aquéllas que sean irrespetuosas u ofensivas o que estén formuladas en un idioma distinto al español, sin la traducción correspondiente.

Esta es una manera de aplicar el principio de máxima publicidad y de que la autoridad facilite el acceso a la información, la traducción impuesta en los casos de los idiomas distintos al español puede o debe ser subsanada por el sujeto obligado o por el propio Instituto, sobre todo considerando que en Chiapas puede formularse en lenguas indígenas. Tener la posibilidad de contar con traductores de las instituciones educativas podría ser una solución a este tema. Habrá que hacer la modificación correspondiente respecto a esta exigencia. La calificación de irrespetuosa u ofensiva también parece un requisito innecesario en la ley, en tanto que implica solicitar información de manera respetuosa y no ofensiva. La autoridad debe centrarse únicamente en la naturaleza de la información requerida.

Respecto al plazo de entrega de la información solicitada, Chiapas se encuentra con 30 días de plazo máximo, estando por encima de Querétaro que tiene 50 días, y en rango con algunos otros estados como Campeche, Baja California Sur, Coahuila, Guerrero entre otros, pero deberá de considerar el plazo de 15 días que tiene Baja California; Hidalgo 18 y Puebla 20[26].

Este aspecto puede mejorarse, ya que el plazo para resolver la solicitud de información es amplio y al existir legislaciones que contemplan un plazo menor, se abre el reto para bajar el tiempo de respuesta, abriendo la posibilidad de duplicar el término cuando la información solicitada no sea de fácil acceso para el sujeto obligado.

Ahora bien, las leyes de acceso a la información pública tienen como finalidad la de garantizar plenamente la transparencia del servicio público, en qué gasta la administración pública y demás poderes, los recursos que obtienen; pero asimismo da la posibilidad de que exista información que puede ser reservada por la autoridad y otra que se clasifique como confidencial.

Hay que destacar que estos dos conceptos aunque parezcan idénticos son distintos, ya que tienen diferentes finalidades. La reserva de la información procede de forma temporal, es decir, que se encuentra restringida al público por un tiempo establecido. Según la ley local, este tipo de información será restringida en los siguientes casos:

---

[26]Métrica de la transparencia 2012. *Op cit*. Pag.33

- Cuando se trate de información, cuya divulgación ponga en riesgo la seguridad del Estado y la seguridad pública;
- La que comprometa la seguridad, la vida o la salud de cualquier persona;
- Cuando su divulgación pueda causar perjuicio a las actividades de prevención o persecución de los delitos, el desarrollo de investigaciones privadas, la impartición de justicia, la recaudación de las contribuciones;
- La generada por la realización de un trámite administrativo, que por el estado que guarda, se requiera mantener en reserva hasta la finalización del mismo;
- La que refiera a expedientes de procesos jurisdiccionales o de procedimientos administrativos, seguidos en forma de juicio, en tanto, no hayan causado estado, en los términos de esta Ley;
- Cuando la información trate sobre estudios y proyectos, cuya divulgación pueda causar daños al interés del Estado, o suponga un riesgo para su realización;
- Cuando la información consista en cuestiones industriales, comerciales, financieras, científicas, técnicas, invenciones y patentes, que fueran recibidas por un órgano del Estado y su revelación perjudique o lesione los intereses generales;
- Cuando se trate de información correspondiente a documentos o comunicaciones internas, que sean parte de un proceso deliberativo previo a la toma de una decisión administrativa; o se trate de un procedimiento

administrativo en el que no se haya perfeccionado el acto administrativo que se persigue;

- Cuando la información pueda generar una ventaja personal indebida en perjuicio de un tercero;
- La de particulares, recibida por los sujetos obligados con el carácter de reservada;
- La que se refiere a los datos individuales de las personas, arrestadas como presuntos responsables de la comisión de algún delito, hasta antes de que sea resuelta la sanción administrativa o la sentencia respectiva.
- Los expedientes, archivos y documentos que se obtengan producto de las actividades relativas a la prevención, que llevan a cabo las autoridades en materia de seguridad pública y procuración de justicia en el Estado y las averiguaciones previas.
- La que se encuentra clasificada por disposición expresa de otra ley, como de acceso prohibido o restringido.

Estas limitaciones al derecho de información son muy similares, por no decir que son idénticas a la de las demás entidades federativas, ya que toman como marco regulatorio la documentación que a nivel federal es considerada de reserva, ajustándose cada ley solamente a su circunscripción.

Hay que destacar que la legislación del estado de Chiapas establece que el término respecto de la información clasificada como de reserva, no puede exceder del plazo de 6 años, debiendo en su oportunidad ser accesible para la ciu-

dadanía, pudiendo ser, por causas justificadas, prorrogada por un periodo idéntico, siempre y cuando el sujeto obligado acredite ante el órgano de control la necesidad de continuar con reserva dicha información.

En este punto, el plazo de duración de la confidencialidad sí es diferente en las demás entidades federativas, ejemplo de esto es el Distrito Federal que el plazo es de 7 años, mientras que en Sinaloa es de 8.

Por otro lado, la información clasificada como confidencial tiene que ver con documentos que por su manejo y divulgación este protegida por el derecho fundamental a la privacidad y que haya sido circunscrita únicamente a los servidores públicos que la deban conocer en razón del ejercicio de sus funciones, como por ejemplo, los datos personales de los empleados de gobierno.

La legislación chiapaneca contempla como información confidencial la siguiente:

- Aquella que se refiera a datos personales y que requieran el consentimiento expreso de las personas para su publicación, distribución o comercialización y cuya divulgación no se encuentre prevista en una Ley.
- La que refiera al patrimonio de personas morales de derecho privado.
- La relacionada con el derecho a la vida privada, honor y la propia imagen.
- La información que se encuentre protegida por la le-

> gislación en materia de derechos de autor o propiedad intelectual.

Este tipo de información no estará sujeta a ningún plazo de vencimiento, por lo que siempre será considerada como secreta, por la gravedad de su divulgación. Debo destacar que en la legislación del estado de Sinaloa, considera como información confidencial la que se desprenda de información personal como nombre de personas, credo, dirección, orientación sexual, etcétera, siendo sancionada la divulgación de esta información por las autoridades.

Por otra parte, con independencia de lo previsto en el artículo 22 de la ley en estudio, el silencio de los sujetos obligados no se interpretará como negativa de una solicitud de información, sino como un acto de incumplimiento de obligaciones, en el que, en su caso, incurrirían servidores públicos adscritos a los mismos; lo que deberá sancionarse conforme a la Ley de Responsabilidades de los Servidores Públicos del Estado.

Ahora bien comentando el segundo párrafo de este artículo, respecto a la negativa ficta, conserva la fórmula de la ley original misma que fue cuestionada en su oportunidad por LIMAC como una solución legal que limita el derecho de acceso a la información porque el recurso no puede ser interpuesto y se desvía el propósito de la norma a la responsabilidad de los servidores públicos.

En Chiapas originalmente la ley contó con un sólo re-

glamento; sin embargo con una reforma reciente, como ya apuntamos, se estableció un criterio distinto, lo que no contribuye con el principio de máximo acceso a la información; ya que disperso la regulación administrativa en diversos reglamentos según el sujeto obligado, lo que impone al sujeto de derecho el deber de consultar en cada caso, los diversos ordenamientos administrativos.[27]

SU GRADO DE DESARROLLO

Para hablar acerca del desarrollo del marco jurídico vigente en el estado de Chiapas, tomaremos como referente, que en 2010, el "Centro de Investigación y Docencia Económicas (CIDE), llevó a cabo el estudio Métrica de transparencia 2010 (MT)3, el cual permitió elaborar un diagnóstico de la situación actual del derecho de acceso a la información en México a partir de un análisis extensivo y minucioso de marcos normativos, instituciones garantes, portales de transparencia, operadores y procesos de acceso a la información pública, así como el Código de Buenas Prácticas[28].

---

[27]Artículo 23.- Los sujetos obligados, en el ámbito de sus respectivas competencias, establecerán, mediante reglamento o acuerdos de carácter general, los órganos, criterios y procedimientos para proporcionar a los particulares el acceso a la información pública, de conformidad con las bases y principios establecidos en ésta.

[28]López Ayllon coord. 2007. El Código de Buenas Prácticas y Alternativas para el Diseño de Leyes de Transparencia y Acceso a la Información Pública es una propuesta que, producto de un ejercicio de consulta y consenso, expone en un

Los resultados de ese estudio proporcionan un diagnóstico completo del funcionamiento del sistema de transparencia en México, en los ámbitos federal, estatal y municipal, en los poderes ejecutivo, legislativo, judicial, los órganos autónomos (institutos electorales, comisiones de derechos humanos y órganos garantes de transparencia) y organismos descentralizados (DIF y organismos operadores de agua). Este artículo utilizara los datos arrojados por este análisis serio, que permite comparar y ubicar con detalle la situación del actual marco jurídico en la entidad. La evaluación de un cuerpo normativo, seguramente tiene en este estudio un importante precedente para evaluar otros ordenamientos legales.

Los indicadores utilizados para realizar el análisis de la legislación de la materia[29], en diversos estudios elaborados son, mismos que fueron en su momento reprobados por la Ley de Transparencia de Chiapas en su primera versión,

formato propio de un instrumento legislativo, las mejores prácticas en materia de acceso a la información y protección de datos personales, así como alternativas concretas para el diseño de las leyes de acceso a la información pública en México, todo ello de manera congruente con los principios y bases que contiene el texto reformado del artículo 6° constitucional. El Código desarrolla así una serie de prácticas que pretenden servir como un marco de referencia para el diseño de las legislaciones en materia de transparencia y acceso a la información pública.

[29]A fin de que los mandatos del artículo 6° constitucional sean una realidad, no basta con las reformas a las leyes de transparencia y acceso a la información, sino que es recomendable emprender una revisión integral del marco jurídico en materia de información, especialmente en las áreas fiscal, administrativa, penal, electoral y de responsabilidades, a fin de dar congruencia constitucional al conjunto de los ordenamientos que, de manera directa o indirecta, se ven afectados por el ejercicio del derecho fundamental de acceso a la información.

verbigracia: sujetos obligados, definiciones, interpretación, información de oficio, límites al derecho de acceso a la información, versiones públicas, máxima publicidad, prueba de daño, gratuidad de la información, periodo de reserva, formas de solicitud de acceso a la información, hábeas data o protección de datos personales, órgano garante, afirmativa ficta, vías de impugnación, formas de control de la ley, y ámbito temporal de validez.

Los objetivos que se propuso ese análisis fueron: "extraer de la realidad legislativa elementos que permitan cuantificar ciertas características medibles del sistema jurídico mexicano en materia de acceso a la información pública; identificar los principales indicadores legales de acceso a la información pública, de acuerdo con estándares reconocidos internacionalmente (Organización de Estados Americanos) y a los principios fundamentales del derecho de acceso a la información pública (recapitulados por la sociedad civil y expertos en la materia); y comparar el contenido normativo de las leyes del sistema jurídico mexicano en materia de acceso a la información pública para establecer la jerarquía en el cumplimiento de los rangos determinados.

En este estudio, el Estado de Chiapas sale con la siguiente puntuación en los aspectos medidos, por cierto bien evaluado respecto a la media nacional. No obstante, hay que subrayar que el propio estudio advierte que esta evolución se hizo en un perspectiva de mediano y largo plazo que considera que en el proceso de implantación de estas políticas

requiere necesariamente de un proceso de maduración jurídica, organizacional e institucional"[30]. Sobre ese estado de maduración jurídica es que haremos unos comentarios sobre los desafíos de la legislación de nuestra entidad.

El estado de Chiapas según la Tabla 1. Valores por entidad por dimensión en materia de desarrollo de la normatividad en materia de transparencia y acceso a la información pública fue calificado con un puntaje de 0.733, relativamente debajo del promedio nacional que tiene un puntaje de 0.762 así como de la legislación federal que tiene un dato de 0.806; en materia de desarrollo y servicio que prestan portales electrónicos para hacer accesible el derecho alcanzó una calificación 0.897, arriba del promedio nacional de 0.778 y de nuevo debajo del puntaje federal de 0.961; en el caso del resultados con usuario simulados su resultado fue importante porque superó con 964 al promedio nacional de 821 y de la federación 911; respecto al desarrollo de capacidades institucionales Chiapas tuvo un promedio de 0.734 superando la media nacional de 0.566 y de la Federación 0.693[31]. Con estos datos el propio estudio ubica a Chiapas en el número 21 respecto al desarrollo de la normatividad, en el lugar número 6 de los portales y el privilegiado segundo lugar de usuario simulado.

[30]*Op Cit*. Pág., 3

[31]Las bases de datos que sustentan cada una de las secciones se encuentran disponibles en el sitio de internet www.metricadetransparencia.cide.edu

Debemos apuntar que en Chiapas en el ejercicio 2012 se abrió paso a las solicitudes de acceso a la información pública a través del sistema electrónico: INFOMEX Chiapas, que es una herramienta utilizada por las personas para realizar con gran facilidad solicitudes de información pública y en su caso, interponer recursos de revisión al inconformarse con las respuestas de los sujetos obligados. Esto significa que ahora las personas pueden ejercer su derecho de acceso a la información pública sin tener que acudir a las oficinas para solicitar datos, es decir, sólo con el uso de Internet puede obtener la información que requieran. Cabe señalar que esta incorporación tecnológica demuestra la voluntad de facilitar el acceso, no obstante, se hace después que muchos estados y la propia federación. (vale hacer mención de que la mayor parte de la población no tiene acceso a recursos tecnológicos, por lo que es una medida que puede dar resultado en las cabeceras municipales o las principales ciudades de Chiapas y no así en toda la entidad).

Para tener una idea como participa la ciudadanía de nuestro estado que tiene aproximadamente una población de 4 796 580 habitantes, tenemos el dato de que el año antepasado, 2012 a través del sistema INFOMEX Chiapas, se recibieron 2 mil 215 solicitudes de acceso a la información pública en el Estado de Chiapas, mismas que se distribuyeron de la siguiente manera: el Poder Ejecutivo recibió 996, el Poder Judicial 310, el Poder Legislativo 85, los Órganos Autónomos 384 y 13 de los 122 Municipios recibieron 440

solicitudes de igual en este mismo periodo se interpusieron 67 recurso de revisión. Para compáralo con un estado que inicio antes la vigencia de su ley como Sinaloa donde INFOMEX reporta para el año pasado un total de solicitudes 3,876 y 87 recurso de revisión interpuestos en una población de 2 767 761 habitantes un poca más de la mitad de la población de Chiapas. Para tener otro de dato de referencia del lugar más desarrollado en la cultura del ejercicio de ese derecho, por ser la capital del país con casi 8 851 080 habitantes tuvo durante el 2012 un total 91,576 solicitudes.

> El sistema INFOMEX para solicitar información a diferentes dependencias gubernamentales o sujetos obligados, según la Ley de Acceso a la Información Pública, reporta únicamente 33 mil 07 cuentas dadas de alta desde la creación del Instituto de Acceso a la Información Pública de Chiapas (IAIP) en 2006, de acuerdo a información de esta dependencia. Si el porcentaje se sacara en relación al número de habitantes la proporción sería mucho menor, de 0.06% de los casi 5 millones de chiapanecos que registra el INEGI en la entidad. En el segundo aspecto, el número de solicitudes que se tramitan en promedio es de 5.5 diariamente o 167 cada mes de acuerdo a los informes de 2008 a 2012 que son los únicos que están disponibles en el portal del IAIP. Así, en los últimos cinco años el IAIP ha recibido un total de diez mil 34 solicitudes de información siendo dirigida la mayoría a los poderes Ejecutivo, Legislativo y Judicial, seguido de los organismos autónomos y municipios. En este tercer aspecto, el número de solicitudes ha variado de manera inestable en esos años, pues un año sube mientras que el siguiente baja tal como lo muestran las cifras de dichos informes: 2008,

mil 747; 2009, 2 mil 553; 2010, mil 944; 2011, 2 mil 175 y 2012 con mil 615.[32]

DESAFÍOS DE LA LEY

Debemos advertir que la expedición de una ley no es suficiente para generar las condiciones democráticas de la observancia de los principios del derecho de acceso a la información. Es fundamental desarrollar las condiciones objetivas y subjetivas de operación, para poder corroborar la eficacia en el ejercicio del derecho y también ponderar su grado de evaluación a partir del proceso de implementación de todo el sistema de protección jurídica e institucional de este derecho.

Hay una marcada tendencia de la legislación de algunos países y en algunas entidades federativas, están regulando en ordenamientos independientes los temas del acceso y la protección de los datos personales. El legislador chiapaneco deberá considerar esta posibilidad con el propósito de mejorar el marco jurídico actual.[33]

La legislación local de Chiapas en la materia, podría incorporar que la información pública en poder de particu-

[32]Eduardo Grajales. En pañales la transparencia en Chiapas. http://www.revistauniversa.com/articulo/en-panales-la-cultura-de-transparencia-en-chiapas/

[33]Métrica. pág.13. Finalmente debe considerarse que existe una tendencia creciente a expedir, en forma independientes a leyes de transparencia y acceso a la información, leyes de datos personales y leyes de archivos.

lares[34] sea considerada también como un elemento que debe proporcionársele a quien la solicite, al igual que lo contempla la actual Ley Federal denominada de esa manera. Incluir a otros entes de naturaleza privada que manejan información pública estatal cuando esta posesión se deriva.

También podría considerar la inclusión de los partidos políticos como sujetos obligados directos, lo cual implica la obligación de éstos de contar con oficinas de información pública para responder a los cuestionamientos de las personas respecto al origen y destino de los recursos públicos que reciben, así como otras cuestiones que puedan interesar a la población[35].

El sistema de nombramiento del órgano garante debe ser mediante un procedimiento democrático y buscar que quienes lo representen tengan una formación suficiente en los distintos campos que implican el conocimiento del tema, políticas públicas, derecho de la información y derecho informático, trasparencia de la gestión, teoría política y teoría del estado.

El programa de difusión debe provocar que la ciudadanía participe solicitando información, cuestión que hasta

---

[34]Mariana Cendejas Jáuregui. Breve análisis de la nueva Ley de Transparencia y Acceso a la Información Pública del Distrito Federal. "Por otro lado, se establece que toda persona moral, señalando a organizaciones de la sociedad civil, sindicatos o cualquier otra análoga que reciban recursos públicos por cualquier concepto, a excepción de las cuotas sindicales, debe proporcionar a los entes públicos de los que reciban recursos, la información relativa al uso, destino y actividades que realicen con éstos".

[35]*Ob cit*, Mariana Cendejas Jáuregui. Breve análisis de la nueva Ley de Transparencia y Acceso a la Información Pública del Distrito Federal.

la presente fecha indica que poco se ha ocupado esta instancia para conseguirla. Las estadísticas actuales demuestran poca demanda de información y poco ejercicio del derecho. Poco desarrollo de la cultura de la transparencia entre los funcionarios públicos.

Podríamos incluir diagramas de flujo para ilustrar el proceso solicitud de información y otro para ilustrar la accesibilidad a través del portal en Chiapas.

Incluir algo de INEGI acerca de las estadísticas que ellos manejan en cuanto a accesibilidad a recursos tecnológicos (con computadora sólo el 12.6 de la población general y con internet apenas el 7.2; ocupamos el lugar número 32 en la escala nacional); para ilustrar que en la realidad del estado el portal no es funcional.

Además el 89.4% de la población es analfabeta, por lo que deberían buscarse estrategias para permitir a esa población acceder al derecho de forma oral y no escrita.

*ADDENDUM

Cabe destacar que el 24 de diciembre de 2014, mediante Decreto número 143, se reformó la Ley, misma que hasta hoy se encuentra vigente y es aplicable a la materia.

Los preceptos que sufrieron modificaciones fueron: Artículo 2, respecto de la obligatoriedad de la Ley; artículos 60, 61, 62 y 63, relacionados con la conformación del Ins-

tituto de Acceso a la Información Pública, pasando nuevamente de cinco a tres consejeros e instituyéndolo como un órgano autónomo especializado, imparcial, colegiado, con autonomía técnica, presupuestal y administrativa; artículo 66 y 67, por los que se establece la figura de un Contralor Interno y sus facultades; y por último los artículos relacionados con el recurso de revisión.

REFERENCIAS

CARPIZO, Jorge y Villanueva, Ernesto, "El derecho a la información. Propuestas de algunos elementos para su regulación en México", en Valadés, Diego y Gutiérrez Rivas, Rodrigo, Derechos humanos. Memoria del IV Congreso Nacional de Derecho Constitucional III, México, Universidad Nacional Autónoma de México, 2001.

CARBONELL, Miguel, "La reforma constitucional en materia de acceso a la información: una aproximación general", en Bustillos, Jorge y Carbonell, Miguel (coords.), *Hacia una democracia de contenidos: la reforma constitucional en materia de transparencia,* México, InfoDF, IFAI, UNAM, 2007.

CENDEJAS JÁUREGUI, Mariana, *Derecho a la información y Poder Judicial*, tesis doctoral, España, Universidad Complutense de Madrid, 2006.

GÓMEZ GALLARDO, Perla y VILLANUEVA, Ernesto, *Indicadores legales y reforma al artículo 6o. constitucional*, LIMAC, *http://www.limac.org.mx/migracion/files/Indica dores.ppt, 8 de agosto de 2008.*

LÓPEZ-AYLLÓN, Sergio, "La reforma y sus efectos legislativos. ¿Qué contenidos para la nueva generación de leyes de acceso a la información pública, transparencia y datos personales?, en Salazar Ugarte, Pedro (coord.), *El derecho de acceso a la información en la Constitución mexicana: razones, significados y consecuencias*, México, IFAI, UNAM, 2008.

MERINO, Mauricio, "Muchas políticas y un solo derecho", en López-Ayllón, Sergio (coord.), *Democracia, transparencia y Constitución. Propuestas para un debate necesario*, México, IFAI, UNAM, 2006.

NAVA GOMAR, Salvador, "Información reservada", en Villanueva, Ernesto y Luna Pla, Issa (eds.), *Derecho de acceso a la información pública. Valoraciones Iniciales*, México, UNAM, 2004.

SALAZAR UGARTE, Pedro y VÁZQUEZ SÁNCHEZ, Paula, "La reforma al artículo 6o. de la Constitución Mexicana: contexto normativo y alcance interpretativo", en Salazar Ugarte, Pedro (coord.), *El derecho de acceso a la información en la Constitución mexicana: razones, significados y contenidos*, México, UNAM, IFAI, 2008.

RAMÍREZ León, Margarita Lucero. Alcances y limitaciones de la Ley federal de transparencia y acceso a la información

pública: una mirada desde la perspectiva de la transición a la democracia México Editorial Universidad Iberoamericana,Año 2003

VILLANUEVA, Ernesto, *Derecho de acceso a la información pública en Latinoamérica*, México, UNAM, 2003.

THOMAS S. Blanton, Ernesto Villanueva, Kate Doyle, coordinadores. Derecho de acceso a la información pública en América. Sinaloa, México. Editorial Universidad de Occidente. 2003.

DE LA ROCHA Dorangélica El derecho de acceso a la información pública y su impacto en los estados de México. Una perspectiva desde la experiencia de Sinaloa (artículo) http://www.juridicas.unam.mx/publica/librev/rev/decoin/cont/4/art/art6.pdf México, Instituto de Investigaciones Jurídicas, UNAM.2004

CONTRATOS ELECTRÓNICOS UNA APROXIMACIÓN A SU REGULACIÓN EN EL MARCO JURÍDICO MEXICANO Y ESPAÑOL

I.- INTRODUCCIÓN

Como es sabido, el proceso globalizador que surgió con la caída de las economías centralmente planificadas, ha generado una serie de transformaciones que no sólo se constriñen al ámbito económico, sino también al político, tecnológico, laboral, cultural y social; es decir toda actividad que se desprende del quehacer humano, se ha visto trastocada por este fenómeno. Aunado a lo anterior, la masificación de la Red denominada *ARPANet* en su origen, conocida actualmente como *Internet,* ha provocado que las personas físicas o morales, modifiquen su forma de relacionarse, alterando con esto la vida social.

El advenimiento de las tecnologías de la información y las comunicaciones o *TICS,* entendidas como "sistemas tecnológicos mediante los que se recibe, manipula y procesa información y que facilitan la comunicación entre dos o más interlocutores" (CEPAL, 2003), ha ocasionado la migración de las actividades hacia la digitalización; lo que se busca es

conformar una sociedad en la que la información sea considerada como un derecho inalienable al ser humano, generando igualdad de oportunidades que propicien y generen condiciones para reducir la brecha social que caracteriza a las sociedades actuales. Julio Téllez Váldes (2004) nos habla de una "*sociedad de la información incluyente*, que habilite a todas las personas libremente y sin distinción de ningún tipo para crear, recibir, compartir y utilizar información y conocimientos que permitan promover su desarrollo económico, social, cultural y político".

En este contexto, han surgido una serie de interrogantes que atañen al derecho; éste como disciplina orientada a regular la actividad humana, ha debido modificarse para responder a las necesidades sociales. A partir de la digitalización de diversos sectores, tales como el comercio, se han planteado una serie de reformas que posibiliten al Estado proporcionar certeza jurídica a los involucrados en el proceso; sin embargo debido a las características propias de Internet, como la deslocalización, inexistencia de regulación específica, multiplicidad de funciones e inmaterialidad de soportes, entre otros, se ha dificultado encontrar la solución adecuada.

El presente trabajo se da en el marco del Curso de Especialización en Contratos y Daños, impartido en la Universidad de Salamanca y busca retratar el panorama actual que guarda el tema del contrato electrónico dentro del orden jurídico mexicano y español, que por el momento se encuentra focalizado en el sector comercial, pero que seguramente

y según las tendencias actuales, permeará en todos los demás sectores, obligando al legislador a adaptar el entramado legal a las exigencias de la realidad digitalizada.

CAPÍTULO I
COMERCIO ELECTRÓNICO

El comercio electrónico, definido por la Organización para la Cooperación y el Desarrollo Económico (2000), como la "compra o venta de bienes o servicios, ya sea entre empresas, hogares, individuos, gobiernos, y otras organizaciones públicas o privadas, realizadas a través de redes computacionales. Los bienes y servicios se ordenan a través de esas redes, pero el pago y la entrega final pueden ser realizadas en o fuera de línea", tuvo sus primeros indicios en ventas realizadas por televisión, en ellas se ofertaban bienes por catálogo que atraían a los consumidores a partir del realismo que implicaba observar las características del producto exaltadas de forma visual, la orden y pago se realizaban generalmente por vía telefónica y con cargo a alguna tarjeta de crédito.

La situación del comercio electrónico desde ese entonces hasta ahora ha variado indudablemente, la apertura de mercados aunada a la explosión tecnológica, ha permitido que se pase de ventas contadas en miles de pesos a las que superan los millones de dólares.

El Estudio de Comercio Electrónico 2013 realizado por la Asociación Mexicana de Internet (AMIPCI, 2013) estimó que el comercio electrónico en México presentó un incremento del 42% respecto del año 2012, generando una derrama económica de 121.6 mil millones de pesos; la tendencia de crecimiento es cada vez mayor, si tomamos en cuenta que durante el año 2004, las ventas totales del comercio electrónico al consumidor ascendían a 2,384 millones 687 mil pesos (AMIPCI, 2005)[1].

Son muchas las ventajas que el comercio electrónico brinda, tanto a vendedores u ofertantes como a los consumidores; entre las características que el proveedor considera valiosas, se encuentran la disminución en los costos de producción, ya que permite ofrecer servicios sin necesidad de contar con una plantilla numerosa, además de no precisar un espacio físico determinado para las ventas; la exhibición del producto puede permanecer las 24 horas los 365 días del año, dando lugar a posibles ventas; la apertura de mercados internacionales sin necesidad de traslado, así como la agilidad en los tiempos y costos de operación.

[1]Según datos estadísticos obtenidos de la página oficial del Instituto Nacional de Estadística y Geografía, (INEGI), existen alrededor de 46,026,450 usuarios de internet, de los cuales el 64.3% utiliza el recurso con la finalidad de buscar información, y el resto de los usuarios se encuentran distribuidos entre comunicación, entretenimiento, apoyo a la educación y capacitación, redes sociales, operaciones bancarias en línea e interacción con el gobierno. Cabe mencionar que por cada rubro, el usuario puede formalizar uno o varios contratos electrónicos para que el producto o servicio le sea proporcionado por el proveedor correspondiente, aun cuando no exista una transacción monetaria o comercial en juego.

Los clientes, por su lado, consideran razones válidas para realizar compras *on-line*; la optimización en el tiempo de compra, lo que permite agilizar el proceso, el abaratamiento en los costos, la posibilidad de encontrar mayor variedad de productos y/o servicios, la entrega a domicilio de los productos solicitados, además de que la oferta no sólo se limita al producto nacional, sino que abarca el internacional; sin embargo, a pesar de las múltiples ventajas que este servicio representa, así como del crecimiento acelerado que muestra este sector, además de los controles y métodos de fomento a la confianza del consumidor implementados por las empresas, entre los que se encuentran, según el informe citado, las certificaciones de calidad; políticas de devolución, garantías y/o cancelación; login y password; privacidad de datos personales, entre otros, la desconfianza del consumidor aún es elevada y continúa siendo un factor determinante para la compra, así como un reto para el legislador que deberá brindar los instrumentos jurídicos necesarios que otorguen certeza a las partes.

En este tenor, se han realizado varios intentos, tanto nacionales como internacionales, para generar instrumentos jurídicos que regulen, no sólo los intercambios, sino toda la actividad que se genera a partir de Internet. A este efecto, la Comisión de las Naciones Unidas para la Unificación del Derecho Mercantil Internacional, aprobó en junio de 1996 la Ley Modelo cuyo principal objetivo fue que:

> ...mediante el establecimiento de un marco jurídico uniforme e internacionalmente aceptable que brindara seguridad jurídica en el uso de las tecnologías electrónicas en la transacciones comerciales entabladas a través de redes de comunicación tanto cerradas como abiertas al público en general, eliminar los obstáculos jurídicos que se generan en las comunicaciones electrónicas con motivo de la aplicación de los requisitos de forma pero sin prescindir de su función básica

Asimismo en julio de 2001, se expidió la Ley Modelo para las Firmas Electrónicas, que ya había sido regulada por el orden jurídico español, a través del Real Decreto-Ley 14/1999 de 17 de septiembre, y que sería sustituida por la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Por su parte el legislador mexicano, por medio del decreto publicado el 29 de mayo de 2000, tuvo a bien reformar y adicionar diversas disposiciones del Código Civil para Distrito Federal en Materia Común y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio, y de la Ley Federal de Protección al Consumidor; éstas reformas tuvieron como objetivo principal regular cuestiones relativas al comercio electrónico, así como a la contratación electrónica, ya que como bien sabemos, el contrato es y seguirá siendo "uno de los pilares básicos del orden económico, pues a través de él se realiza la función de intercambio de los bienes y servicios" (Díez-Picaso y Gullón, 2012).

En este contexto, la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales, aprobada el 23 de noviembre de 2005, ofrece, en palabras de la Secretaría de la Comisión de las Naciones Unidas para el Derecho Mercantil, soluciones prácticas para las cuestiones que plantea la utilización de medios electrónicos de comunicación para la celebración de contratos internacionales. Ésta es aplicable entre contratantes que empleen medios electrónicos y se encuentren en distintos Estados, aun cuando no sean Estados Contratantes de la Convención, por ello la relevancia de su existencia[2].

La Unión Europea, a través de la Comisión de las Comunidades Europeas, presentó durante el año de 1997, la Iniciativa europea de comercio electrónico cuya finalidad fue fomentar el crecimiento del comercio electrónico en Europa, considerando su impacto en los mercados mundiales. Dicha iniciativa contemplaba un programa de trabajo a concluirse antes de culminar el año 2000, que incluía cuestiones regulatorias, entre las que destacaban, la puesta en marcha de reglamentación en el ámbito del pago electrónico, los contratos negociados a distancia para servicios finan-

[2]Cabe hacer mención que la Convención, si bien es cierto, trata de unificar los criterios respecto de la forma que deberán adoptar los contratos, cumplimiento, ámbito de aplicación y requisitos de validez, no tiene como objetivo regular cuestiones de derecho sustantivo que tienen que ver con la formación de los contratos y de los derechos y obligaciones de las partes, esa parte deberá ser normada por el derecho interno del país.

cieros, los derechos de propiedad intelectual, la protección de los servicios de acceso condicional y la firma digital; así como la evaluación de la necesidad de adoptar nuevas iniciativas en relación a derecho de contratos, uso fraudulento del pago electrónico, seguridad y protección de datos, entre otros. Derivado de esta iniciativa se aprobaron la Directiva 2000/31/CE del Parlamento Europeo y del Consejo de 8 de junio de 2000, relativa a determinados aspectos jurídicos del comercio electrónico en el mercado interior, Directiva 1999/93/CE de 13 de diciembre de 1999 por la que se establece un marco común para la firma electrónica, Recomendación 97/489/CE de la Comisión, de 30 de julio de 1997, relativa a las transacciones efectuadas mediante instrumentos electrónicos de pago, en particular, las relaciones entre emisores y titulares de tales instrumentos, Directiva 97/7/CE, de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia, entre muchas otras acciones que se orientaron a fortalecer el comercio y contratación electrónica.

En lo que se refiere al marco jurídico español, existen diversas disposiciones que regulan, tanto el comercio electrónico como la contratación electrónica, entre las más destacadas se encuentran, la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, que se apega a las disposiciones de la Directiva 2000/31/CE; Real Decreto 1163/2005, de 30 de septiembre, por el que se regula el distintivo público de confianza en

los servicios de la sociedad de la información y de comercio electrónico, así como los requisitos y el procedimiento de concesión; Real Decreto 1906/1999, de 17 de diciembre, por el que se regula la contratación telefónica o electrónica con condiciones generales en desarrollo del artículo 5.3 de la Ley 7/1998, de 13 de abril, de condiciones generales de contratación, éste aplica a contratos realizados de forma telefónica, electrónica o telemática; Real Decreto–Ley 14/1999, de 17 de septiembre, sobre firma electrónica; Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, que surgió a partir del Plan Avanza aprobado en 2005, además de otras que en lo subsecuente se tratarán.

Es por ello, que en lo sucesivo analizaremos los elementos básicos de la contratación electrónica, los tipos de contratos electrónicos que existen, el marco regulatorio español y el mexicano, tratando de establecer un comparativo entre ambos órdenes y planteando desafíos y estrategias para consolidar la contratación electrónica.

CAPÍTULO II
LA CONTRATACIÓN ELECTRÓNICA Y SU REGLAMENTACIÓN EN EL ORDEN JURÍDICO MEXICANO

Como es sabido, la principal fuente de obligaciones, encuentra su fundamento en el contrato, éste adquiere relevancia cuando existe un acuerdo de voluntades entre dos o más

sujetos, sobre un negocio u objeto particular, que tiene por objeto crear, transmitir o extinguir derechos y obligaciones.

El Código Civil Federal por su parte, hace una distinción entre convenio y contrato, éste enuncia:

> Artículo 1792.- Convenio es el acuerdo de dos o más personas para crear, transmitir, modificar, o extinguir obligaciones.
>
> Artículo 1703.- Los convenios que producen o transfieren las obligaciones y derechos, toman el nombre de contratos.

Encontramos pues, que el legislador opto por diferenciar ambas figuras siguiendo lo acotado por Hans Kelsen en su obra *El contrato y el tratado*; en ella establece que la palabra contrato entraña dos sentidos; el primero se refiere al contrato como el acuerdo en el que existe un pacto que da origen a ciertos efectos jurídicos, y el segundo corresponde a la coerción con carácter de norma que adquiere al ser celebrado voluntariamente por las partes.

En la actualidad y debido a las transformaciones que constantemente sufre la actividad humana, la concepción clásica de contrato ha cambiado; en primer lugar, cuando nos referimos a un acuerdo hemos de decir que ambos contratantes se encuentran en igualdad de circunstancias, es decir, que existe una especie de equilibrio que impide que alguno de ellos se encuentre en desventaja, situación que en la actualidad es difícil de conseguir, ya que existe una terrible desigualdad generada por la acumulación de riqueza en

las manos de algunos grupos, quienes generalmente son los que determinan las condiciones de contratación, dejando a los consumidores la única opción de adherirse (contratos de adhesión) a las clausulas determinadas por ellos en beneficio de sus intereses; tal es el caso de las instituciones bancarias, los grandes corporativos, las compañías telefónicas, los proveedores de servicios, entre tantos otros.

Por tanto, ha de ser función del Estado, garantizar las condiciones que permitan a los consumidores actuar en una posición no tan desventajosa. Luis Diéz-Picazo (2012), propone algunos aspectos que debe contemplar la intervención estatal para equilibrar el actuar de los contratantes, entre los que se encuentran:

1. Limitación del principio de la libertad de contratar. Cuando los agentes económicos gozan de supremacía en el mercado...

2. Limitación del principio de libertad en la fijación del contenido del contrato, que lleva al establecimiento con normas de ius cogens de la trama que constituyen los derechos y deberes de las partes para hacer posible la igualdad entre las mismas...

3. Fijación imperativa de los precios de bienes o servicios o sometimiento de ellos a un control público.

La modernidad y las nuevas tecnologías han hecho que surjan nuevas formas de celebrar un contrato, que aunque

obedecen a los principios emanados de la teoría general del contrato, reúnen características especiales que modifican la manera en la que se expresa la voluntad, éstos al igual que cualquier contrato deben reunir los elementos esenciales, que se encuentran descritos en el artículo 1794 del Código Civil Federal:

> Artículo 1794.- Para la existencia del contrato se requiere:
>
> I. Consentimiento
> II. Objeto que pueda ser materia del contrato

Con la reforma llevada a cabo el 29 de mayo de 2000, el legislador realizó modificaciones al artículo 1803 del Código en mención, ésta tuvo la finalidad de incluir al medio electrónico, óptico o tecnológico dentro de las opciones pertinentes para manifestar la voluntad, quedando como sigue:

> Artículo 1803: El consentimiento puede ser expreso o tácito, para ello se estará a lo siguiente:
>
> I. Será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos.

Debe decirse que aunque el contrato electrónico no se encuentre definido como tal en nuestra legislación, esta modificación da pie a su formación; ya que como anteriormente comentamos, éste no representa una nueva clasificación,

sino que se pacta, otorga o formaliza a través de medios distintos a los tradicionales.

Respecto de la exigencia en cuanto a la forma para el contrato, cabe decir que el artículo 1834 bis, modificado también durante el año 2000, determina que para los contratos que requieran plasmarse por escrito y que deban ser firmados, podrán tenerse como satisfechos los mencionados requisitos, a través de la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, siempre y cuando la información generada o comunicada pueda atribuirse a las personas obligadas y sea accesible para consultas posteriores.

Ahora bien, es importante destacar que para que un contrato se forme es necesario que exista una oferta y su correspondiente aceptación, al respecto el Código dispone: "Artículo 1807.- El contrato se forma en el momento en el que el proponente reciba la aceptación, estando ligado por su oferta, según los artículos precedentes."

Entonces se deduce que el contrato es perfecto y surte sus efectos legales, a partir del momento mismo en el que la propuesta aceptada es recibida por el ofertante, sin embargo cuando existen elementos que pueden influir o variar respecto del momento de aceptación, el legislador considera algunas limitantes, descritas en lo sucesivo:

> Artículo 1804.- Toda persona que propone a otra la celebración de un contrato, fijándole un plazo para aceptar, queda ligada por su oferta hasta la expiración del plazo

> Artículo 1805.- Cuando la oferta se haga a una persona presente, sin fijación de plazo para aceptarla, el autor de la oferta queda desligado si la aceptación no se hace inmediatamente. La misma regla se aplicará a la oferta hecha por teléfono o través de cualquier otro medio electrónico, óptico o de cualquier otra tecnología que permita la expresión de la oferta y la aceptación de ésta en forma inmediata.
>
> Artículo 1806.- Cuando la oferta se haga sin fijación de plazo a una persona no presente, el autor de la oferta quedará ligado durante tres días, además del tiempo necesario para la ida y vuelta regular del correo público, o del que se juzgue bastante, no habiendo correo público, según las distancias y la facilidad o dificultad de las comunicaciones.

De lo anterior, se desprende que al tratarse de ofertas hechas por medios electrónicos, la aceptación tendrá que darse de manera inmediata; sin embargo, algo que se desea destacar en el presente trabajo, es que según lo determinado por el artículo 1806, las ofertas realizadas a personas ausentes se mantienen firmes durante tres días, y en el caso de medios electrónicos resulta obvio que las partes se encuentran ausentes o es prácticamente imposible determinar el momento en el que la oferta es vista por el receptor, elemento que al parecer no fue considerado por el legislador en la reforma de mayo de 2000, para precisar la duración de la propuesta.

Ahora bien, es de importancia hacer notar que los contratos electrónicos definidos por Juan Carlos Villalba

(2008) como "aquellos que engloban a los contratos que se perfeccionan mediante el intercambio electrónico de datos de ordenador a ordenador", cuentan con características propias, que pueden resumirse del siguiente modo:

• La contratación electrónica se produce a través de dispositivos o medios electrónicos o digitales, llámense así, teléfonos, computadoras, tabletas, televisores, fax, consolas de videojuegos, cajeros automáticos, etc.

• Generalmente no son plasmados en un soporte papel, ya que se celebran a partir de un medio desmaterializado, que en raras ocasiones exige la conservación del documento en un soporte material, no digitalizado.

• Las partes contratantes en muchos casos se encuentran ausentes, y pocas veces existe la posibilidad de ubicarlas físicamente.

• El lugar para la celebración de los contratos electrónicos es un espacio deslocalizado, no existe una ubicación física determinada, a no ser las de las personas que intervienen en la contratación.

• Existe una clara reducción en los tiempos de operación, tanto de los ofertantes como de los consumidores.

• El intercambio de bienes o servicios que se da a partir de la celebración del acto, generalmente no pasa por controles fronterizos o aduaneros.

• El medio en el que operan es una red abierta.

• Se crean nuevos riesgos que pueden influir o modificar las condiciones de la contratación o la manifestación de

la voluntad, debidas al tráfico constante en el intercambio de datos, la multiplicidad de usuarios existentes, la posibilidad de que los archivos sean borrados, la carencia de soportes físicos, la existencia de virus, entre otros.

En tal virtud, podríamos decir entonces, que el contrato electrónico es el acuerdo que se establece a través de medios informáticos o electrónicos, que tiene por objeto crear, transmitir o extinguir derechos y obligaciones, caracterizado por la deslocalización del medio, la ausencia de las partes y de soportes físicos o materiales que hagan patente lo pactado.

En este tenor podemos argumentar que debido a las características propias del contrato, éste puede verse afectado, con mayor frecuencia que cualquier otro, de causas o vicios que puedan invalidarlo.

El artículo 1795 establece como causas de invalidez del contrato, las siguientes:

> I.- Incapacidad legal de las partes o una de ellas
> II.- Vicios del consentimiento
> III.- Objeto, motivo o fin ilícito
> IV.- Falta de forma en la manifestación del consentimiento, cuando la ley así lo establezca.

Si tomamos en cuenta que a través del medio electrónico, es difícil verificar no sólo la identidad de los contratantes, sino también la sustancia de la cosa objeto del contrato, además de la imposibilidad de juzgar acerca de los motivos o

fines que conducen la voluntad de los contratantes, y la poca disponibilidad de elementos técnicos para dar formalidad al negocio, es de especial importancia hallar los mecanismos que den mayor certeza y seguridad para la realización del acto.

Supongamos que nos encontramos en un supuesto en el que uno de los contratantes es menor de edad o actúa ostentando una personalidad que no es la propia, además adquiere un producto que se ofrece en el sitio web de una empresa X, y al recibirlo se percata de que se trata de uno con características diferentes a las ofrecidas, por otro lado el producto adquirido es objeto de un robo con violencia y desafortunadamente no cuenta con un soporte físico o digital de lo pactado en días anteriores, debido a un corte eléctrico que causo fallas en el equipo que almacenaba la información.

Ante un ambiente tan adverso, es preciso tomar en cuenta al menos los siguientes elementos al momento de contratar:

• Solicitar los documentos que puedan acreditar la identidad del contratante, en el caso de una persona física, alguna identificación oficial que pueda coincidir con los datos de la cuenta a la que se va a realizar el cargo, el Registro Federal de Contribuyentes y de ser posible la plena identificación a través de alguna cámara web, en la que se capture la pantalla asociando el rostro de quien aparece con la identificación proporcionada; para el caso de las personas morales,

es prudente solicitar los datos de constitución y registro, así como su identificación y domicilio fiscal.

• Solicitar la información correspondiente de los servicios que oferta, que deberán coincidir con el objeto social de la misma.

• Verificar que el servicio o producto requerido, corresponda con el deseado u ofertado, exponiendo de forma clara, precisa, escrita y almacenable para ulteriores consultas, las características técnicas, físicas, cualitativas o cuantitativas que reúne y de ser posible anexar una fotografía del mismo.

• Acordar el lugar en el que se tendrá por celebrado el contrato, que puede tratarse del domicilio del ofertante o del consumidor.

• Obtener datos acerca del momento en el que se tiene por perfeccionado el contrato, es decir el momento en el cual se formaliza, que generalmente se da al presionar la tecla para aceptar o firmar de modo digital el documento.

• Solicitar el acuse de recibo y el documento por escrito que contenga todas las condiciones y clausulas a que se obligan los contratantes.

• Guardar el documento en dos o tres dispositivos de almacenamiento que permitan su revisión posterior, y de ser posible imprimirlo para contar con un soporte material que pueda servir como medio de prueba en caso de conflicto.

Con respecto al último punto, nuestro Código Federal de Procedimientos Civiles contempla en su artículo 210-A, producto de la reforma del 2000, lo siguiente:

> Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.
>
> Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.
>
> Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta.

Como puede observarse, la ley es especialmente cuidadosa en recalcar que para que la información pueda ser considerada como prueba, deberá ser obtenida a través de dispositivos confiables, además de ser atribuible a quienes se obligaron; sin embargo en ningún momento determina el Código, la forma en la que la información habrá de ser generada para poder ser atribuida. En paralelo, la reforma del 29 de mayo, abarcó también modificaciones al Código de Comercio, en el que sí se observa un mecanismo que permite presumir la procedencia de la misma.

> Artículo 90.- Salvo pacto en contrario, se presumirá que el mensaje de datos proviene del emisor si ha sido enviado:
>
> I.- Usando medios de identificación, tales como claves o contraseñas de él, o
>
> II.- Por un sistema de información programado por el emisor o en su nombre para que opere automáticamente.

Hago la aclaración que por mensaje de datos, el legislador estipuló que se trata precisamente de la información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o de cualquier otra tecnología.

De cualquier modo es conveniente comentar que un mensaje de datos, también debe reunir determinadas características que permitan confiar de forma plena acerca de su origen, Julio Téllez Valdés (2004) las clasifica de la manera siguiente:

I.- Autenticidad
II.- Integridad
III.- No repudiación o rechazo

La primera claramente se refiere a la determinación que pueda hacerse acerca de la procedencia del mensaje, es decir poder verificar la identidad de quien lo envía; la segunda hace hincapié a que el mensaje comunique justamente la información que se desea, que no se halle alterado de forma alguna y que antes de concretar el contrato se verifi-

que que en efecto se trata del negocio pactado; y la tercera característica radica en el hecho de que no existan causas que puedan anular lo contratado y originar desacuerdos entre lo pactado y lo entregado.

Es importante mencionar que, de acuerdo a la reforma llevada a cabo el 29 de agosto de 2003, el Código de Comercio establece en su artículo 93, al igual que el Código Civil para el supuesto, que:

> Cuando la ley exija la forma escrita para los contratos y la firma de los documentos relativos, esos supuestos se tendrán por cumplidos tratándose de mensaje de datos siempre que éste sea atribuible a las personas obligadas y accesible para su ulterior consulta...

De enorme valor es entonces, determinar que para que un mensaje de datos sea confiable deberá, entre otras cosas, firmarse electrónicamente de algún modo, cuanto mejor si a través de un prestador de servicios de certificación, se expide un certificado acerca de la veracidad de la firma que se está plasmando.

En este tenor fue que el legislador, tomando en cuenta la infinidad de supuestos que pueden viciar o anular un contrato o desvirtuar cualquier información que sea almacenada, generada, enviada o recibida a través de un mensaje de datos, fue que el 29 de agosto de 2003, publicó el Decreto por el que se reformaron los artículos 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108,

109, 110, 111, 112, 113 y 114, y se adicionaron los artículos 89 bis, 90 bis, 91 bis y 93 bis, así como los Capítulos Primero, Segundo, Tercero y Cuarto al Título Segundo, denominado del Comercio Electrónico.

La reforma incluía, entre otras cosas, la definición de conceptos tales como; certificado, datos de creación de firma electrónica, firma electrónica, firma electrónica avanzada o fiable, mensaje de datos y prestador de servicios de certificación; además de precisar el momento en el que se considera recibido un mensaje de datos, así como su respectivo acuse, característica de especial relevancia en los contratos, ya que indica el momento en el que el consentimiento se hace patente, originando que se perfeccione y cause por ende todos sus efectos legales.

De igual modo, incorporó lo relativo a la firma electrónica y los prestadores de servicios de certificación, dándoles facultades para tal fin, a los notarios públicos y corredores públicos, a las personas morales de carácter privado y a las instituciones públicas.

Es pertinente pues, para los fines de este trabajo argumentar que la firma electrónica es realmente el factor que puede generar la confianza requerida para resolver de forma positiva cualquier negocio electrónico, ésta es equiparable a la firma autógrafa y puede, a través de ella, presumirse que el contratante, en efecto es quien está llevando a cabo el acto, dando con eso validez al contrato.

Al respecto, cabe decir que el Código de Comercio, la

define como "los datos en forma electrónica consignados en un mensaje de datos, o adjuntados lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información contenida en el mensaje de datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio".

Es significativo hacer notar que el mismo Código establece una diferenciación entre firma electrónica y firma electrónica avanzada o fiable; al respecto enuncia:

> Firma Electrónica Avanzada o Fiable: Aquella Firma Electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97.
>
> Artículo 97.- Cuando la ley requiera o las partes acuerden la existencia de una Firma en relación con un Mensaje de Datos, se entenderá satisfecho dicho requerimiento si se utiliza una Firma Electrónica que resulte apropiada para los fines para los cuales se generó o comunicó ese Mensaje de Datos.
>
> La Firma Electrónica se considerará Avanzada o Fiable si cumple por lo menos los siguientes requisitos:
>
> I. Los Datos de Creación de la Firma, en el contexto en que son utilizados, corresponden exclusivamente al Firmante;
>
> II. Los Datos de Creación de la Firma estaban, en el momento de la firma, bajo el control exclusivo del Firmante;
>
> III. Es posible detectar cualquier alteración de la Firma Electrónica hecha después del momento de la firma, y

> IV. Respecto a la integridad de la información de un Mensaje de Datos, es posible detectar cualquier alteración de ésta hecha después del momento de la firma.
>
> Lo dispuesto en el presente artículo se entenderá sin perjuicio de la posibilidad de que cualquier persona demuestre de cualquier otra manera la fiabilidad de una Firma Electrónica; o presente pruebas de que una Firma Electrónica no es fiable.

Es útil decir que la firma electrónica tiene, en un ambiente con las peculiaridades que ya describimos, un valor trascendental; por tal motivo y a pesar de las medidas de seguridad que puedan ser utilizadas en la creación de la misma, el Código puntualiza que las consecuencias jurídicas que entrañe el hecho, serán responsabilidad del Destinatario y de la Parte que Confía, en caso de que no se hayan tomado las medidas necesarias para:

> I. Verificar la fiabilidad de la Firma Electrónica, o
>
> II. Cuando la Firma Electrónica esté sustentada por un Certificado:
>
> a) Verificar, incluso en forma inmediata, la validez, suspensión, o revocación del Certificado, y
>
> b) Tener en cuenta cualquier limitación de uso contenida en el Certificado.

Todo lo anterior se debe a que, como ya se dijo anteriormente, para que un negocio jurídico pueda llevarse a

cabo y prosperar, es necesario que impere un ambiente de confianza; propósito que se cree fue el motivo principal del legislador, para la aprobación de la serie de reformas hechas en los años 2000 y 2003, que fueron el producto de una serie de cambios internacionales tendentes a promover el comercio electrónico.

En este orden de ideas y precisamente por ser el consumidor, en muchas ocasiones, el menos favorecido es que se reformaron y adicionaron algunos artículos a Ley Federal de Protección al Consumidor, que incluyeron a las transacciones llevadas a cabo a través de medios electrónicos, ópticos o de cualquier otra tecnología como objeto de protección de la Ley; además de imponer al proveedor, la obligación de proporcionar al consumidor, su domicilio físico, números telefónicos, entre otros medios, para efecto de presentar quejas, reclamaciones o aclaraciones relacionadas con el negocio llevado a cabo; así como la determinación de la facultad por parte del consumidor, de conocer toda la información acerca de los términos, condiciones, costos, cargos adicionales y formas de pago de los bienes y servicios provistos; características que considero son de especial importancia en la formalización de un contrato, ya que como se dijo en líneas anteriores, otorgan certeza jurídica al consumidor.

Además de lo citado, se consideraron aspectos relacionados con la protección de los datos personales del consumidor, instituyendo un registro a cargo de la Procuraduría

del Consumidor, al que deberán inscribirse quienes no deseen que su información sea utilizada con fines mercadológicos o publicitarios.

En ese tenor fue que la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, determinó que cualquier persona que recolecte o almacene datos personales, deberá dar el aviso de privacidad[3] al titular de la información para que éste otorgue el consentimiento a efecto de que sus datos sean manejados o no. La Ley es clara al establecer que el consentimiento por parte del titular podrá darse de forma escrita, verbal o por medios electrónicos, ópticos o de cualquier otra tecnología, o en su caso por signos inequívocos.

CAPÍTULO III
MARCO JURÍDICO ESPAÑOL

En lo que respecta al marco jurídico español, podemos decir que el antecedente más certero, que encabezó la serie de transformaciones legales, relacionadas con la Sociedad de la Información fue la Directiva 2000/31/CE del Parlamento Europeo y del Consejo del 8 de junio de 2000, ésta tuvo como finalidad, crear un marco jurídico en el que los servicios de

[3]Por aviso de privacidad se entiende, para efectos de la Ley, "aquel documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales.

la Sociedad de la Información pudieran circular libremente entre los Estados miembros, entendiendo al desarrollo del comercio electrónico como un motor capaz de generar crecimiento a nivel local, a través de la potenciación de la pequeña y mediana empresa, favoreciendo así a la industria europea y por ende produciendo condiciones que permitirían al mercado europeo competir con cualquier otro.

La Directiva hace alusión a una serie de características que deben reunir las actividades económicas desarrolladas en línea para ser consideradas como conformadoras de la Sociedad de la Información, denotando que las actividades no sólo se limitan a los servicios que dan lugar a la contratación en línea, sino también a aquellos que representan una actividad económica como, el ofrecimiento de información, comunicación búsqueda, acceso y recopilación de datos en línea.

Establece la obligación de los Estados miembros de adecuar su legislación, respecto de los requisitos, principalmente formales, de la contratación por vía electrónica, enunciando que las adecuaciones deberán hacerse conforme al régimen jurídico relativo a los contratos, consagrado en el Derecho Comunitario.

En la Sección tercera, destinada a los contratos por vía electrónica, puntualiza que los Estados miembros, pueden disponer adecuar o no su legislación respecto de la contratación electrónica, cuando se trate de contratos que sean incluidos en las siguientes categorías:

a) los contratos de creación o transferencia de derechos en materia inmobiliaria, con la excepción de los derechos de arrendamiento;

b) los contratos que requieran por ley la intervención de los tribunales, las autoridades públicas o profesionales que ejerzan una función pública;

c) los contratos de crédito y caución y las garantías presentadas por personas que actúan por motivos ajenos a su actividad económica, negocio o profesión;

d) los contratos en materia de Derecho de familia o de sucesiones.

Además, alista una serie de datos que los prestadores de servicio deberán proporcionar al consumidor, entre las que se encuentran: las condiciones generales de contratación, los códigos de conducta a los que deberá apegarse el actuar de los contratantes, los medios técnicos de los que se dispone para la corrección de errores y las lenguas ofrecidas para la celebración del contrato.

De igual modo constituye a la solución extrajudicial de conflictos como una alternativa para la solución de controversias en materia de contratación electrónica y determina que en caso de incumplimiento podrán hacerse acreedores a sanciones que deberán ser efectivas, proporcionadas y disuasorias, determinadas por los Estados miembros.

Fue entonces, que a raíz de la mencionada Directiva, se promovieron y promulgaron una serie de leyes, y decre-

tos que integran ahora el marco normativo español, respecto de comercio electrónico y contratación electrónica.

De entre todos ellos, describiremos los siguientes cuerpos normativos:

La Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, tuvo por objeto incorporar al ordenamiento jurídico español, las disposiciones de la Directiva 2000/31/ CE del Parlamento Europeo y del Consejo, en ella se regulan las cuestiones relativas a los servicios de la sociedad de la información y contratación electrónica, que no se encuentran plenamente identificados por los demás cuerpos normativos españoles, ya sean generales o especiales, y que por lo novedoso del medio electrónico, no fueron contempladas en el pasado.

La aplicabilidad de la ley, se da para los prestadores de servicios establecidos en España, y para aquellos que sin ser residentes prestan servicios clasificados como de la sociedad de la información, que cuenten con un establecimiento permanente en España. Relevante es que para efectos de la ley, se entiende por establecimiento "el lugar desde el que se dirige y gestiona una actividad económica", que generalmente es el conocido domicilio fiscal, hecho de especial importancia al momento de determinar leyes y autoridades adecuadas para aplicar la ley.

Además estipula que la ley será aplicable, aun cuando se trate de un prestador de servicios establecido en cual-

quier otro Estado de la Unión Europea, pero que haya prestado servicios de la sociedad de la información a un residente español, detallando las materias que deberán verse afectadas y que son las siguientes:

> a) Derechos de propiedad intelectual o industrial
>
> b) Emisión de publicidad por instituciones de inversión colectiva
>
> c) Actividad de seguro directo, realizada en régimen de derecho de establecimiento o en régimen de libre prestación de servicios
>
> d) Obligaciones nacidas de los contratos celebrados por personas físicas que tengan la condición de consumidores.
>
> e) Régimen de elección por las partes contratantes de la legislación aplicable a un contrato
>
> f) Licitud de las comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente no solicitadas.

Algo particularmente novedoso, radica en la provisión que se hace respecto a la inscripción en el Registro Público del nombre o nombres de dominio de Internet, correspondientes al prestador de servicios; lo anterior con la finalidad de facilitar a los ciudadanos y a la Administración Pública, la accesibilidad a los datos de quien está ofreciendo el servicio.

Al igual que la Directiva 2000/31]/CE, la Ley establece que los prestadores de servicios deberán tener especial

atención en colocar de forma accesible y en la página de Internet que ostenta, toda la información relativa a la empresa, las condiciones generales de contratación, los costos precisos y la posibilidad de imprimir y archivar los derechos y obligaciones a que se están sometiendo.

Determina también, todo lo relacionado a condiciones generales de contratación electrónica y a la validez y eficacia de los contratos electrónicos, aclarando que también regirán para la materia, el Código Civil y el Código de Comercio, así como las restantes normas mercantiles o civiles, en especial, las de protección a los consumidores y usuarios y de ordenación de la actividad comercial.

En cuanto a la forma exigida para ciertos actos, la Ley determina que si se trata de la documental pública, o que requieran de órganos jurisdiccionales, notarios, registradores de la propiedad y mercantiles o autoridades públicas, se estará a lo dispuesto por su legislación específica.

La entrada en vigor de esta Ley, modifico lo relativo a regulación sobre contratación telefónica o electrónica, contenida en el Real Decreto 1906/1999, de 17 de diciembre, para adecuar su contenido a las disposiciones contenidas en la Ley ; así también los Códigos Civil y de Comercio.

La Ley 56/2007 de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, se dio en el marco del Plan Avanza 2006-2010 para el desarrollo de la Sociedad de la Información y de convergencia con Europa y entre Comu-

nidades Autónomas y Ciudades Autónomas, que tiene como objetivo:

> conseguir la adecuada utilización de las TIC para contribuir al éxito de un modelo de crecimiento económico basado en el incremento de la competitividad y la productividad, la promoción de la igualdad social y regional, la accesibilidad universal y la mejora del bienestar y la calidad de vida de los ciudadanos españoles[4] (Plan Avanza, 2005).

En este tenor fue que a partir de la Ley se hicieron importantes modificaciones a lo concerniente a facturación electrónica y firma digital, estableciendo la obligatoriedad de utilizar facturas electrónicas cuando se trate de contratos efectuados con el sector público estatal, además de

[4]El Plan Avanza comprendió cinco ejes de actuación, que tuvieron como finalidad hacer de la economía española una economía competitiva, con niveles de crecimiento elevados, a través de la incorporación de diversas estrategias que la incluían en la era de la información. Las áreas de actuación propuestas en el Plan son:

1.- Hogar e inclusión de ciudadanos, donde se desarrollan medidas para garantizar la extensión del uso de las TIC en los hogares y aumentar y potenciar la inclusión y se amplían los ámbitos de participación de la ciudadanía en la vida pública.

2.- Competitividad e innovación, con medidas encaminadas a impulsar el desarrollo del sector TIC en España y la adopción de soluciones tecnológicamente avanzadas por las PYMEs españolas.

3.- Educación en la Era Digital, incorporando las TIC en el proceso educativo y de formación en general e integrando a todos los agentes que en él participan.

4.- Servicios Públicos Digitales, con medidas que permitan mejorar los servicios prestados por las Administraciones Públicas, aumentando la calidad de vida de los ciudadanos y la eficiencia de las empresas.

5.- El nuevo contexto digital, con el despliegue de infraestructuras de banda ancha que lleguen a todo el país, genere confianza en ciudadanos y empresas en el uso de las nuevas tecnologías, proporcione mecanismos de seguridad avanzados y promueva la creación de nuevos contenidos digitales.

alentar entre las micro, pequeñas y medianas empresas el desarrollo de este tipo de facturación para contribuir de ese modo al fortalecimiento del comercio electrónico.

Además contempla, en el capítulo segundo, una serie de modificaciones a diversas leyes, que tienen como finalidad adecuar la normatividad vigente. Entre las que más nos importan para los fines del presente trabajo, se encuentran, las relativas al valor probatorio de los contratos electrónicos celebrados mediante instrumentos de firma electrónica y la relativa a la información previa que debe brindar el prestador de servicios, obligándolo a adecuar el formato para el medio de comunicación utilizado.

La Ley 30/2007, de 30 de octubre, de Contratos del Sector Público, que observa todo lo relativo a contratación pública, tipos de contratos, duración de los mismos, elementos de validez, forma específica, órganos de contratación, trámites y requisitos para licitación, etc. En lo tocante a la contratación electrónica, se observa la intención de incorporar la digitalización al sector público, a través de figuras, tales como: subasta electrónica, publicidad contractual por medios electrónicos, facturación electrónica, envío de información y documentación a través de medios electrónicos, informáticos o telemáticos.

Conveniente es decir que además de la normatividad descrita, se encuentran también otros cuerpos normativos, que aunque específicamente no determinen pautas o linea-

mientos generales de contratación electrónica, sí determinan elementos, requisitos y peculiaridades que dan pie a la formación del contrato mismo, entre ellas destacan:

• Código Civil español, que como sabemos define al contrato como figura jurídica, enumera los requisitos esenciales para la validez de todos los contratos, que son consentimiento, objeto cierto, causa de la obligación; cuestiones relativas a la interpretación, rescisión y nulidad de los mismos.

• Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista, que tiene por objeto, establecer el régimen jurídico general del comercio minorista, así como regular ventas especiales y actividades de promoción comercial.

• Ley 7/1998, de 13 de abril, sobre condiciones generales de contratación, que como objeto principal tiene, como su nombre lo dice, establecer las condiciones generales de contratación, bajo principios de igualdad, evitar cláusulas abusivas, protección al consumidor, entre otras.

• Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica, cuyo objetivo es regular el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación.

• Real Decreto 1906/1999, de 17 de diciembre, por el que se regula la contratación telefónica o electrónica con condiciones generales en desarrollo del artículo 5.3 de la Ley 7/1998, de 13 de abril, de condiciones generales de contratación.

CONCLUSIONES

• El desarrollo de las tecnologías de la información y el proceso globalizador cada vez más dinámico, ha ocasionado que el derecho, como disciplina encargada de regular la actividad humana y procurar el bien común, se transforme con el objeto de regular la digitalización de los diferentes sectores que integran a nuestra sociedad.

• El comercio electrónico en México, ha aumentado en un 42% respecto del año 2012, lo que ha generado que se lleven a cabo mayor número de actos a través de los contratos electrónicos.

• El legislador preocupado por brindar certeza jurídica a los contratantes, ha tratado de adaptar la legislación existente a las nuevas realidades virtuales; sin embargo el esfuerzo no ha sido suficiente, ya que debido a las particularidades de Internet, los riesgos en la contratación han aumentado considerablemente, provocando en muchas ocasiones que el "acuerdo de voluntades" al que las partes llegan pueda ser inválido o nulo.

• El Código Civil Federal mexicano es el principal ordenamiento que rige sobre la contratación electrónica; existen leyes secundarias como la Ley Federal de Protección al Consumidor y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que norman situaciones específicas respecto de contratación electrónica, más no elementos considerados esenciales para la existencia del acto.

• La legislación española, siguiendo los acuerdos tomados en la Directiva 2000/31/CE del Parlamento Europeo y del Consejo del 8 de junio de 2000, aprobó diversos ordenamientos que regulan a la contratación por la vía electrónica, entre los que se encuentran, la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, Ley 56/2007 de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información y el Código Civil español entre varios otros.

• La contratación electrónica, es un fenómeno poco explorado, que deberá ser ampliamente estudiado, para que a través de mecanismos legales, tales como la firma electrónica avanzada, y los recursos propios de Internet; las video llamadas, los sistemas de almacenamiento de datos y de seguridad, pueda darse en un ambiente de confianza y certeza jurídica para las partes.

REFERENCIAS

García, C.T., (2009). Reflexiones en torno a la Teoría General del Contrato. *Revista de Derecho Privado, 21-22, 41-67.*

López, V.M., (2010). *Regulación Jurídica de la Contratación Electrónica en el Código Civil Federal.* Toluca: Instituto de Transparencia y Acceso a la Información Pública del Estado de México y Municipios.

Cámara Oficial de Comercio e Industria en Madrid. (2008). *Contratación electrónica.* Madrid: Camerfirma

Villalba, C. J., (2008). Contratos por medios electrónicos. *Prolegómenos. Derechos y Valores. 22, 85-108.*

Téllez, J. (2003). *Derecho Informático.* México. Mc Graw Hill.

Ríos, J.J. (1997). *Derecho e informática en México. Informática jurídica y derecho de la informática*. México. Instituto de Investigaciones Jurídicas

Comisión Económica para América Latina y el Caribe. (2003). *Los caminos hacia una sociedad de la información en América Latina y el Caribe* (Publicación LC/G.2195/Rev. 1-P). Santiago de Chile: Organización de las Naciones Unidas.

Código Civil Federal. H. Congreso de la Unión. Cámara de Diputados, LXII Legislatura. Información Parlamentaria.

Código de Comercio. H. Congreso de la Unión. Cámara de Diputados, LXII Legislatura. Información Parlamentaria.

Código Federal de Procedimientos Civiles. H. Congreso de la Unión. Cámara de Diputados, LXII Legislatura. Información Parlamentaria.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares. H. Congreso de la Unión. Cámara de Diputados, LXII Legislatura. Información Parlamentaria.

Ley Federal de Protección al Consumidor. H. Congreso de la Unión. Cámara de Diputados, LXII Legislatura. Información Parlamentaria.

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Agencia Estatal Boletín Oficial del Estado. Ministerio de la Presidencia. Gobierno de España.

La Ley 56/2007 de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información. Agencia Estatal Boletín Oficial del Estado. Ministerio de la Presidencia. Gobierno de España.

Ley 30/2007, de 30 de octubre, de Contratos del Sector Público. Agencia Estatal Boletín Oficial del Estado. Ministerio de la Presidencia. Gobierno de España.

Código Civil Español. Agencia Estatal Boletín Oficial del Estado. Ministerio de la Presidencia. Gobierno de España.

Ley 7/1996, de 15 de enero, de Ordenación del Comercio Minorista. Agencia Estatal Boletín Oficial del Estado. Ministerio de la Presidencia. Gobierno de España.

Ley 7/1998, de 13 de abril, sobre condiciones generales de contratación. Agencia Estatal Boletín Oficial del Estado. Ministerio de la Presidencia. Gobierno de España.

Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica. Agencia Estatal Boletín Oficial del Estado. Ministerio de la Presidencia. Gobierno de España.

Real Decreto 1906/1999, de 17 de diciembre, por el que se regula la contratación telefónica o electrónica con condiciones generales en desarrollo del artículo 5.3 de la Ley 7/1998, de 13 de abril, de condiciones generales de contratación. Agencia Estatal Boletín Oficial del Estado. Ministerio de la Presidencia. Gobierno de España.

Este libro se terminó de editar en diciembre de 2015,
en Austin, Texas; Estados Unidos de Norte América.