



**UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO**

**FACULTAD DE DERECHO**

**DIVISIÓN DE ESTUDIOS DE POSGRADO**

**CIUDAD UNIVERSITARIA**

***DATOS PERSONALES Y SEGURIDAD DE LA  
INFORMACIÓN DEL  
SECTOR EMPRESARIAL EN MÉXICO***

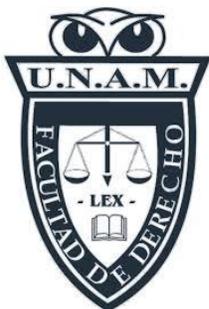
**T E S I N A**

QUE PARA OBTENER EL GRADO DE

***ESPECIALISTA EN DERECHO EMPRESARIAL***

**P R E S E N T A**

**DIANA MÁRQUEZ CISNEROS**



**ASESOR DE TESINA: DRA. CRISTINA CÁZARES SÁNCHEZ**

**MÉXICO, DISTRITO FEDERAL MAYO 2015**



Universidad Nacional  
Autónoma de México

Dirección General de Bibliotecas de la UNAM

**Biblioteca Central**



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

# Dedicatorias

*A Dios, quien es el que pone en nosotros así el querer como el hacer por su buena voluntad (Filipenses 2:13) ya que sin Él, nada de esto hubiera sido posible.*

*A mis padres José Miguel Márquez Rubio y María Cisneros García, por todo su amor, esfuerzo y apoyo. De quienes aprendí a amar la vida, a tener siempre una ilusión y seguir adelante. Gracias por hacer de mí una gran persona. Los amo.*

*A mi hija Tiana Fredel Palencia Márquez, que representa una fuente de constante inspiración y al tenerla entre mis brazos simplemente me di cuenta que mi vida sería mejor que antes, ya que desde ese momento se ha convertido en la razón de mi existir. Te amo hija.*

*A mi hermana Linda Márquez Cisneros y su esposo César Benny González Pérez †, que en todo momento confiaron en mí, estando siempre a mi lado, brindándome incondicionalmente su amor y apoyo.*

*A la memoria de mi amado esposo Jorge Ricardo Palencia Hinojosa †, que a pesar de que no se encuentra físicamente, siempre ha estado en espíritu conmigo.*

*A mis hermanos Belem Melody, Itzel Stephanie y José Miguel quienes han creído en mí y me han ofrecido la calidez de la familia a la cual pertenezco.*

*A mi asesor: Dra. Cristina Cázares Sánchez por su constante apoyo y compromiso.*

## ÍNDICE GENERAL

	Pág.
DEDICATORIAS.....	II
INTRODUCCIÓN.....	VI

### CAPÍTULO PRIMERO

#### EL DERECHO ANTE LAS NUEVAS TECNOLOGÍAS

1.1. La influencia del uso de la tecnología en la vida cotidiana.....	14
1.2. La sociedad de la información.....	19
1.2.1. El Siglo XIX y la Revolución Industrial.....	20
1.2.2. El Siglo XX, inicio de toda una era de evolución científica y tecnológica.....	20
1.2.3. La era digital: a la luz de una evolución e influencia en la vida cotidiana del hombre.....	21
1.3. Las herramientas de la Internet: un desafío para la práctica jurídica.....	24
1.3.1. El correo electrónico.....	26
1.3.2. Los grupos de noticias.....	27
1.3.3. Máquinas de búsquedas.....	27
1.4. El orden público digital: un necesario replanteamiento de juridicidad.....	30
1.5. Usos y costumbres virtuales: un acotamiento a las exigencias axiológicas y técnico-gramaticales. Casos Particulares:.....	32
1.5.1. Sociedad de Información Crediticia.....	36
1.5.2. Instituto Nacional Electoral.....	38
1.5.3. Otras Bases de Datos.....	40
1.5.4. Sector Salud.....	41
1.5.5. Sector Educativo.....	44
1.5.6. Sector de Telecomunicaciones.....	45
1.5.7. Internet.....	47
1.5.8. Redes Sociales: Facebook.....	48

### CAPÍTULO SEGUNDO

#### DATOS PERSONALES Y COMUNICACIÓN PÚBLICA EN MÉXICO

2.1. Comunicación Pública, Espacio Público y Democracia.....	52
2.2. Los Medios de Comunicación como Espacio Público.....	57

2.3. Políticas Públicas y Medios de Comunicación.....	59
2.4. La Protección de Datos Personales en los Medios de Comunicación.....	66
2.5. Los Datos Personales en las Organizaciones y las Políticas de Comunicación Internas.....	71
2.6. Aspectos Generales.....	73

## **CAPÍTULO TERCERO**

### **ASPECTOS JURÍDICOS DE SEGURIDAD DE LA INFORMACIÓN: MEDIDAS DE CUMPLIMIENTO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN EL SECTOR EMPRESARIAL**

3.1. Tecnología y Derecho: Un paso al mundo jurídico virtual.....	74
3.2. Problemas jurídicos derivados de las comunicaciones en línea.....	76
3.3. La conciencia de riesgo en el sector Empresarial.....	78
3.4. Elementos necesarios para la existencia de las obligaciones en línea.....	79
3.5. Implicaciones de una ley en materia de protección de datos personales en las Empresas.....	80
3.6. La protección de datos en el ámbito de la mercadotecnia.....	89
3.7. Las 5 claves para cumplir con la Ley Federal de Protección de Datos Personales por parte de las Empresas.....	93
3.7.1 Crear una carpeta de cumplimiento y el Departamento de Protección de Datos.....	95
3.7.2 Capacitación al interior de la Organización.....	95
3.7.3 El Aviso de Privacidad.....	96
3.7.4 Derechos ARCO.....	97
3.7.5 Medidas de seguridad.....	102
3.8. El cumplimiento de la LFPDPPP se considera un gasto más que una inversión en las Empresas.....	103
3.9. La previsión como estrategia.....	105

## CAPÍTULO CUARTO

### UNA SEMBLANZA SOBRE DERECHO Y PROTECCIÓN DE DATOS PERSONALES: HACIA UNA MODERNIZACIÓN DE LA ENSEÑANZA

4.1. Necesidad e inclusión en la currícula de la Especialización en Derecho Empresarial.....	108
4.2. Enseñar la asignatura de Protección de Datos Personales y seguridad de la información en los actuales planes de estudio.....	109
4.3. Propuesta para la incorporación de la asignatura de Protección de Datos Personales en la Especialidad de Derecho Empresarial.....	112
4.4. Riesgos de las Empresas con la fuga de información.....	113
<b><u>CONCLUSIONES</u></b> .....	117
<b><u>FUENTES DE CONSULTA</u></b>	
A. <b><u>BIBLIOGRÁFICAS</u></b> .....	126
B. <b><u>NORMATIVAS</u></b> .....	127
C. <b><u>ELECTRÓNICAS</u></b> .....	127
D. <b><u>OTRAS</u></b> .....	129
<b><u>GLOSARIO</u></b> .....	131

## INTRODUCCIÓN

Tecnología y Derecho, en un principio puede pensarse que son dos cosas muy distantes una de la otra, y sin embargo, parece que conforme avanza el tiempo ambos fenómenos sociales y en consecuencia productos culturales, se hallan más cercanos y vinculados, ello como consecuencia de la aceleración tecnológica y científica que trae aparejado un aumento exponencial del tráfico de información, permitiendo que las relaciones humanas en nuestra vida cotidiana se lleguen a presentar en formas que jamás imaginamos.

Un dato personal es toda aquella información que nos identifica. Va desde el nombre, apellidos, edad, domicilio, teléfono, correo electrónico, identificaciones oficiales, ingresos, hasta información todavía más sensible: tipo de sangre, preferencia sexual, historial clínico, huella digital, creencias religiosas, etcétera. De manera aislada toda esta información podría parecer no tener mayor uso, sin embargo, almacenada en grandes bases de datos constituye una fuente para el desarrollo de cualquier actividad puesto que las instituciones, tanto públicas como privadas, funcionan con información personal y el cruce de datos permite crear perfiles muy completos de las personas. Sin embargo, el uso que hacen de ella no siempre es el apropiado y su seguridad puede ser fácilmente vulnerada, con serias consecuencias para sus titulares.

No es una posibilidad la existencia de la llamada aldea global, sino que más bien representa una realidad de nuestros días, las herramientas que aportan las telecomunicaciones y el Internet como lo señalan Jose Luis Piñar Mañas y Lina Ornelas Núñez <sup>(1)</sup>, son insustituibles a la hora de mejorar la productividad, la conectividad y la competitividad de la sociedad del Siglo XXI, cuentan desde ahora con principios esenciales para desarrollarse con certeza jurídica, con reglas constitucionales explícitas, con reglas más claras para dar tratamiento a datos personales y con un órgano regulador con experiencia que es el Instituto Federal de Acceso a la Información y Protección de Datos (en adelante IFAI), vivimos en un mundo globalizado, no sólo económicamente sino, ante todo, científico y movido por el desarrollo de la tecnología que ha ido quebrantando intimidades y derrumbando fronteras. En ese orden de ideas, siendo abogados Empresariales no podemos abstraernos a los cambios que la realidad nos plantea.

---

(1) PIÑAR, José Luis y ORNELAS, Lina, *La Protección de Datos Personales en México*, México, D.F., Ed., Tirant Lo Blanch México, 2013, p. 422.

En este contexto, en mi experiencia como abogada de Empresa, me he enfrentado a algunos de estos retos que la realidad modificada por la modernidad y que me hubiera gustado que en mi formación profesional se abordara éste y otros problemas, pero no como comentarios aislados de lo que puede suceder en materia de datos personales y seguridad de la información, sino más bien con un enfoque concreto de los problemas jurídicos que se están suscitando en el sector Empresarial.

Considero que el manejo de este tipo de enseñanza no sólo resulta importante en mi investigación, son incluso necesarios para el desempeño profesional, dando valor agregado que ahora como abogados se nos pide, al menos a nivel de Empresa. Durante el desarrollo de la presente tesina acoté el tema y encontré el nombre adecuado, relacionado con el perfil del abogado Empresarial y los requerimientos sociales que en específico la iniciativa privada requiere. Las herramientas para resolver los problemas que van directamente relacionados con la preparación y perfil de los egresados de la especialización, para atender o resolver los problemas que se nos presentan, la verdadera aplicación la conocemos hasta la práctica, existe una gran diferencia entre el deber ser de nuestras clases y la práctica profesional.

Inicialmente pensé que en mi investigación era posible abarcar todos los tópicos que encierra la figura de Datos Personales y Seguridad de la Información en el Sector Empresarial en México, pero al comenzar su estudio, poco a poco me di cuenta que sería necesario señalar el objeto a un problema específico: *En el sector Empresarial la protección de datos personales y seguridad de la información se ha visto como un gasto más que como una inversión y la necesidad e inclusión en la currícula de la Especialización en Derecho Empresarial.*

Cualquiera que sea la rama en la que se desempeñe el abogado requerirá del manejo de técnicas de administración, así como de conceptos multidisciplinarios como la administración y, la estadística, que favorecerán su desempeño: el **tratamiento legítimo**, controlado e **informado**, garantizando la **privacidad y el derecho a la autodeterminación informativa de las personas**, obligando a sus clientes a velar, responder, así como rendir cuentas al titular sobre el tratamiento de sus datos personales, valiéndose de estándares y mejores prácticas, y esquemas de autorregulación.

El sector Empresarial en México no ha podido adaptarse a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, por una parte el desconocimiento y por la otra al considerarla un gasto más que una inversión, sin embargo

su incumplimiento en cualquiera de sus aspectos puede conllevar importantes consecuencias como: Vulneración de los datos personales de clientes, empleados y proveedores; degradación de la imagen de la compañía ante la sociedad y entre los usuarios que vean vulnerados sus derechos y un **cúmulo de sanciones**. El desconocimiento de la ley no exime de su cumplimiento.

Considero que la base para realizar cambios sociales únicamente se puede lograr a través de la educación y la formación de nuevos abogados con un perfil adecuado, con una mayor visión y con herramientas para resolver problemas más amplios, por lo que se propone incluir en la currícula de la Especialización en Derecho Empresarial la materia de Datos Personales, dando privilegio a las materias formativas, que consoliden el desempeño profesional, con bases generales en las que está sustentado nuestro conocimiento, incluyendo las prácticas. Muchas veces encontramos que nuestras leyes son bastas y completas, siendo que lo que falla es su aplicación, tanto por parte del gobierno como de los abogados que lo permitimos, toleramos y en ocasiones encausamos a nuestros clientes.

Para romper el excesivo formalismo, el desconocimiento y trámites excesivos, costosos e innecesarios se requiere una visión que sólo a través de la educación se puede lograr. Como parte del cambio se hace necesario dar a los especialistas Empresariales herramientas para su desempeño profesional, en materias de administración, como la planeación, la estadística, la visión económica de costo-beneficio, la verdadera aplicación de la tecnología.

Consecuencia a lo anterior y en razón de una exigencia metodológica, se adoptó en definitiva como plan expositivo el que a continuación reseñaré:

1º.- Como cuestiones de carácter introductorio, se precisa acerca de cómo la tecnología ha cambiado a la sociedad y de cómo tal problemática y necesidades, obligan a la integración de una nueva rama de las Ciencias Jurídicas en nuestro país, ya denominada: *Derecho de las Nuevas Tecnologías*.

2º.- Se reflexionó acerca de algunos aspectos jurídicos derivados de la utilización de las nuevas tecnologías, a los que le es inherente la profundización de su problemática jurídica, que se presentan como consecuencia de la utilización de los medios electrónicos, ópticos o de cualquier otra tecnología en el tráfico jurídico de todas las personas de Derecho en nuestro país, ello en el ámbito de datos personales y seguridad de la información.

3°.- Se investigó a la luz de la “teoría clásica” las bases de los datos personales y seguridad de la información que, dio pie para el análisis de los elementos tecnológico-jurídicos que están permitiendo la evolución de esta institución jurídica, poniendo de manifiesto primeramente, la necesaria inversión en el sector Empresarial en materia de protección de datos personales, que tomen en cuenta el desarrollo técnico y científico en los actos más comunes de las organizaciones y segundo, desarrollar los argumentos para la inclusión en la currícula de la Especialización en Derecho Empresarial, la convicción en el lector de la influencia que ejerce la evolución doctrinal y la necesidad de que ésta, se adecúe no sólo a los estudios de especialización en la enseñanza del Derecho Empresarial, sino también a los usos y prácticas de las organizaciones.

4°.- En ese tenor, la investigación apuntaba hacia una doble vertiente: por un lado se imponía bosquejar al menos, los contenidos deseables de un programa que implica la enseñanza en materia de Datos Personales y Seguridad de la Información en el Sector Empresarial, y por otro, la necesaria inclusión de la materia en la currícula de la Especialización en Derecho Empresarial.

Por ello, las ideas que se insertan en el presente trabajo representan únicamente algunas *“reflexiones jurídico-doctrinales sobre la enseñanza de la Protección de Datos Personales y Seguridad de la Información en el Sector Empresarial en México”*.

5°.- Ante tal situación, el objetivo de plantear propuestas concretas y acotadas a nuestra realidad nacional, está alineado a las respuestas que surgen de la relación entre el Derecho y la Seguridad de la Información: ¿Por qué es importante una ley de protección de datos personales? ¿Cuál es la situación en México? ¿Quién tiene que cumplir con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (más adelante LFPDPPP) y quiénes son los principales actores? ¿El cumplimiento se considera un gasto más que una inversión en las Empresas?

Así entre preguntas y respuestas en torno a cómo afecta el uso y manejo de datos personales, en el presente estudio pretendo hacer algunas reflexiones acerca de las principales consecuencias jurídicas que se presentan como resultado de hacer uso de datos personales de clientes, empleados y proveedores, en el marco de lo que considero una urgencia de ocuparnos por comprender y regular situaciones jurídicas que derivan del incumplimiento a la regulación.

Ante los repentinos cambios en la forma en que nos comunicamos y en la que vemos al mundo, se ven reflejados necesariamente en nuestra sociedad y por tanto en el campo de las Ciencias Jurídicas, toda vez que el Derecho es un fenómeno social y su contenido, depende necesariamente de la forma en que la sociedad se transforma, lo que trae aparejado el surgimiento de nuevas situaciones jurídicas que nunca imaginamos fueran posibles como: los datos personales son susceptibles de ser extraídos de instituciones bancarias, crediticias, de servicios como televisión por cable, telefonía celular o fija, e incluso de instituciones gubernamentales o paraestatales, entre otros que se detallarán en esta investigación.

Es innegable que la confluencia de las tecnologías de la comunicación e informática al mismo tiempo que abrió nuevas formas de relacionarnos, ha pulverizado las fronteras de la privacidad del ser humano como un todo, y querámoslo o no, nosotros como seres humanos y como profesionales del Derecho, estamos inmersos en esta corriente de repentinos cambios socio-tecnológicos que necesariamente inciden también en el campo de nuestra especialidad: el Derecho.

Por estas consideraciones y en obvio de repeticiones, el presente trabajo de investigación se realizó de forma sistemática, repasa diversas corrientes de los estudios jurídicos desarrollados hasta la fecha en materia de nuevas tecnologías, pero específicamente en tratándose de Datos Personales, y es por ello, que habré de estudiar la legislación y lo que diversos autores especialistas en el tema han abordado y la diferencia entre la visión en la que ellos han hecho sus estudios y mi experiencia como abogada de Empresa y estudiante de la especialización de Derecho Empresarial. Lo que se pretende es delimitar el tema a la visión práctica y herramientas de administración que se requiere en nuestra profesión, en específico como abogados de Empresa.

En consecuencia y para mejor detalle, el lector encontrará en el desarrollo del texto, planteamientos que sugieren la importancia de dar cumplimiento a la LFPDPPP en el sector Empresarial, por lo que encontrará que:

En el marco del **Capítulo Primero**, denominado como “El Derecho ante las Nuevas Tecnologías” se describen los esfuerzos a demostrar los grandes temas sobre la influencia del uso de la tecnología en nuestra vida cotidiana en el marco de la sociedad de la información, mediante el uso de las herramientas de la Internet, y desde luego las consideraciones de la técnica gramatical, ello, sin descuidar la importancia de la tecnología y

la economía, en el marco de la delimitación en materia de Datos Personales y seguridad de la información, esto es: comprender cómo se estudia; cómo se está implementando en las Empresas esta nueva regulación y, cuáles son los principales problemas.

Lo anterior describe a grandes rasgos cómo el fenómeno de la aceleración tecnológica y científica en el intercambio de información, trae aparejado el riesgo exponencial de que los datos personales de los clientes, empleados y proveedores están susceptibles de ser extraídos mediante cualquier medio, permitiendo el establecimiento de vínculos jurídicos en manera que no se pensó fueran posibles. Se encontrará el estudio a casos particulares desarrollados en distintos sectores tanto del ámbito público como privado, tales como: las Sociedades de Información Crediticia, el Instituto Nacional Electoral, el Sector Salud, el Sector Educativo, el Sector de Telecomunicaciones, Internet, Redes Sociales: Facebook; relacionadas con la protección de la información personal y vislumbra el panorama en México con las leyes y políticas establecidas.

En relación al **Segundo Capítulo**, considero que bajo el título “Datos Personales y Comunicación Pública en México”, desarrolla la participación de la comunicación con la construcción de la democracia al ofrecer un espacio público, así como la forma en que contribuye en la creación de las políticas públicas relacionadas con los datos personales y el papel de los medios de comunicación referente a la protección y la privacidad. Este hecho trasciende porque de esta manera los medios pueden contribuir a crear crítica, rebeldía e inconformidad encausadas para analizar el poder.

De la misma manera los sistemas de comunicación (también por otra parte los cerebros, las células, etcétera), los sistemas de conciencia son sistemas operacionalmente cerrados. No pueden tener contacto unos con otros. No existe la comunicación de conciencia a conciencia, ni entre el individuo y la sociedad. Si se quiere comprender con suficiente precisión la comunicación es necesario excluir tales posibilidades (aun la que consiste en concebir la sociedad como un espíritu colectivo). Solamente una conciencia puede pensar (pero no puede pensar con pensamientos propios dentro de otra conciencia) y solamente la sociedad puede comunicar. En los dos casos se trata de operaciones propias de un sistema operacionalmente cerrado, determinado por la estructura <sup>(2)</sup>.

---

<sup>(2)</sup> NIKLAS, Luhmann. Traducción Gaytán Alcalá Felipe. **Notas Críticas. Teoría de sistemas, la autoobservación de la sociedad moderna.** Editorial Alianza. 2002. p. 658.

Así, se bosqueja como es que a todos y cada uno de los aspectos jurídicos derivados de la comunicación y la utilización de las nuevas tecnologías, le es inherente la profundización de los problemas jurídicos, presentados como consecuencia lógica del uso de los medios electrónicos, ópticos o de cualquier otra tecnología, en todas nuestras actividades particulares o con los órganos de carácter público (especialmente la Administración pública nacional), como es el caso de la determinación de la jurisdicción aplicable a los actos jurídicos celebrados a través del Internet, que como había mencionado, van más allá de los simples actos de comercio; o que decir de los elementos necesarios para el surgimiento de las obligaciones “en línea”.

Por otra parte, las Administraciones Públicas no pueden permanecer aisladas y ajenas a las profundas transformaciones que las tecnologías avanzadas de la información y de las comunicaciones están produciendo en todo el mundo, sino que han de integrarse en la Sociedad del Conocimiento, a fin de mejorar la calidad de sus servicios a los ciudadanos y a la sociedad; por lo que se abordará como el insuficiente conocimiento de los medios de comunicación en temas de datos personales puede generar información incorrecta, una situación que puede influir negativamente en la percepción del público o conducirlo a tomar decisiones equivocadas o contraproducentes. Las políticas públicas de protección de datos personales que comenzaron a crearse, fueron en función del sector público puesto que el derecho de acceso a la información pertenece a este ámbito desde donde se dio inicio a la protección de los datos personales.

Los lectores hallarán en el análisis desarrollado en el **Capítulo Tercero**, en la tónica de lo que considero “Aspectos jurídicos de Seguridad de la Información: Medidas de cumplimiento en materia de Protección de Datos Personales en el Sector Empresarial” con el ánimo del convencimiento de que en la “teoría clásica” se abordan los argumentos que llevan a la convicción de la influencia que ejerce la evolución doctrinal y disciplinaria en las Empresas ante el cumplimiento de la regulación, se desarrollan algunas cuestiones sobre la tecnología y el Derecho en su transición hacia el mundo jurídico electrónico; vinculados a los problemas jurídicos que surgen en las comunicaciones en línea que ubican en los revestimientos contractuales, los mensajes de datos como un concepto legal necesario y los elementos necesarios para la existencia de las obligaciones en línea. La conciencia de riesgo en el sector Empresarial.

La necesidad de que las Empresas implementen la ley mediante los usos y prácticas en materia de seguridad de la información, sus implicaciones, la protección de datos en el ámbito de la mercadotecnia y las 5 claves para cumplir con la ley Federal de Protección de Datos Personales. Análisis al problema en el ámbito de seguridad, el incumplimiento de la ley ya que las Empresas consideran un gasto más que una inversión y su previsión como estrategia.

En relación al **Cuarto Capítulo**, denominado “El Derecho y la Protección de Datos Personales y Seguridad de la Información: Hacia una modernización de la enseñanza”, se establecen los argumentos que considero llevan a la convicción de la influencia que ejerce la evolución doctrinal, y la necesidad de que ésta, se adecue a los estudios de posgrado en la enseñanza del Derecho.

En el marco de la necesidad e inclusión en la currícula de la Especialización de Derecho Empresarial. Así las cosas, invito a las Empresas a convencerse, que el futuro no espera a nadie y si hemos de hacer algo para ponernos al día en materia de Protección de Datos Personales, el momento oportuno es aquí y ahora, por tanto mi propuesta entrelaza los grandes tópicos de las Ciencias Jurídicas.

## **CAPÍTULO PRIMERO**

### **EL DERECHO ANTE LAS NUEVAS TECNOLOGÍAS**

#### **1.1. La influencia del uso de la tecnología en la vida cotidiana.**

En años recientes la división y especialización de las ciencias jurídicas se ha hecho un fenómeno común, así el Derecho, se ha hecho cada vez más específico, ante tal evolución, no puede quedar al margen el estudio de fenómenos tecnológicos y científicos que inciden en el ordenamiento jurídico. En efecto, el uso de las computadoras, el Internet, la telefonía celular y otros dispositivos con características distintas a los tradicionales, han cambiado a nuestra sociedad con nuevas formas de comunicarse y de relacionarse, orillando al Derecho a cambiar y/o adaptar su contenido a nuevos fenómenos sociales (entre estos a la ciencia y tecnología), creando dentro de éste nuevos criterios jurídicos que formalizados tomen un lugar en los principios de ordenación conductual, como el “Derecho de las Nuevas Tecnologías”.

Covarrubias <sup>(1)</sup>, en términos generales, sostiene que la revolución tecnológica que se está produciendo desde mediados del siglo pasado tiene igual o mayor trascendencia en la historia que la revolución industrial en el Siglo XIX, que como es sabido, comenzó cuando James Watt concibió el principio de la máquina de vapor de doble efecto. El derecho se creó para regular las complejas relaciones humanas, con el fin de servir a las personas de instrumento de ordenación y defensa de sí misma y de sus intereses. El propósito de la presente investigación es analizar la información relativa a los datos personales y sus mecanismos de protección en el sector Empresarial, cuya facultad consiste en garantizar la transparencia, el derecho de acceso a la información y la seguridad de la misma. En efecto, “... si la literatura se adelantó a la realidad virtual, Internet tomó por sorpresa a teóricos, filósofos, políticos y estudiosos de la comunicación y la cultura...”. Así es como Adriana Malvido <sup>(2)</sup> se confronta con la realidad modificada por el uso de la tecnología y categóricamente, afirma un hecho que ocurre también en el mundo del Derecho: “... la tecnología se nos adelantó...”.

No es óbice a lo anterior, que se deba reconocer que en todo problema que trasciende en el campo del Derecho, éste primero nace y luego viene la reflexión sobre sus implicaciones éticas, sociales, económicas, políticas y desde luego jurídicas; en el presente

---

<sup>(1)</sup> *Apud*, MALVIDO, Adriana, Por la vereda digital, México, CONACULTA, 1999, p. 109.

<sup>(2)</sup> *Íbid*, p. 25.

trabajo, es necesaria la reflexión, comprensión y sensibilización del jurista frente a las nuevas herramientas de la tecnología como lo son: las computadoras, el Internet y demás medios de comunicación (teletipo, telefonía móvil, fibra óptica, teléfono, televisión, telégrafo, etcétera), y como lo fue en su momento, la implementación del telégrafo que como medio judicial fue útil para llevar a cabo las notificaciones, o bien, la adopción del teléfono para la conformación válida del consentimiento, con esto, se dan los primeros pasos tendientes a la incorporación de los avances científicos y técnicos al campo del Derecho, develándose así las posibilidades que los medios técnicos ofrecían para poder crear situaciones de derecho hasta entonces desconocidas.

Por otro lado el vocablo Internet, alude a los recursos capaces de obtener el máximo aprovechamiento del empleo conjunto de la informática <sup>(3)</sup>, el cable y las telecomunicaciones y es actualmente el medio que permite el acceso a una multitud de servicios y de creaciones en un contexto transfronterizo. El Internet existe y funciona como resultado de que millares de usuarios individuales de redes de computadoras que decidieron utilizar un lenguaje común o también llamado **protocolo** <sup>(4)</sup> de transferencia de información para intercambiarla con otras computadoras, las que a su vez se interconectan entre sí; esto representa probablemente la mayor virtud de la “Red” y al mismo tiempo es lo que puede representar su mayor problema por la transferencia de datos.

Hablando en términos estadísticos mencionaré a Malvido <sup>(5)</sup>, para el año 1999 se estimaba que la Internet tendría doscientos millones de usuarios en más de 50 países, y que para el momento en que se presente este estudio habrá poco más de mil millones de cibernautas, y que cada cuatro segundos se conectará un usuario más a la Red; este dato, sin duda expresa la manera en que aumenta el tráfico de información y con él, la posibilidad de relacionarse no solo a nivel personal, sino también jurídico.

---

<sup>(3)</sup> SABOGAL-RUEDA, Alexander, Conceptos Generales de Telemática. [En línea] <[www.uninet.edu/ummet/conferencias/AlexSabogal/tele2.ppt](http://www.uninet.edu/ummet/conferencias/AlexSabogal/tele2.ppt)> [Consulta 17. feb. 2015], quien apunta que la Informática es “... la ciencia que estudia el tratamiento automático y racional de la información...”, este término se acuñó en Francia durante los años 60s como INFORMATIQUE que quiere decir información automática.

<sup>(4)</sup> En materia de nuevas tecnologías, hay también categorías conceptuales propias, como es el caso del **Protocolo**, el cual es considerado como un conjunto de reglas formales que describen la forma en que se transmiten los datos entre dos o más ordenadores, pero especialmente a través de la Red.

<sup>(5)</sup> *Íbidem*, nota a pie (1), p. 23

Quizá la razón de la popularidad de la Internet se debe a que los resultados de su uso son inmediatos, lo cual se traduce en un sentido de libertad absoluta, de lo que da cuenta la expresión “navegar por la Red” (*surf the Web*) <sup>(6)</sup>.

El veloz intercambio de información, ha hecho que el Derecho se muestre lento, por ejemplo, se calcula que hay más de 10 millones de computadoras en todo el mundo de las cuales el 60% se encuentran en los Estados Unidos y están conectadas a Internet y que unos 40,000,000 de personas acceden a este medio y se esperaba que esta cifra se quintuplicara <sup>(7)</sup>, y es que la totalidad resultante de usuarios, hacen del Internet el más extraordinario medio de comunicación que hasta ahora haya existido, debido a que permite intercambiar información en forma instantánea, además de que ha incrementado las posibilidades de realizar nuestras tareas cotidianas, gracias a la suma de la interconexión de equipos informáticos y bases de datos, aunado a la descentralización y crecimiento de las redes informáticas.

Estadísticas del uso de la Internet señalan que en el Distrito Federal, al mes de abril de 2013, el 60.5% de la población de seis años y más es usuaria de Internet, por lo que su tasa de crecimiento promedio anual es de 9.0%, en el periodo 2010-2013.

En la entidad, el 67.3% de los usuarios de Internet tienen entre 6 y 34 años.

Del total de hogares en el Distrito Federal, el 50.2% cuentan con Internet, esto es, una tasa de crecimiento promedio anual de 10.9% en el periodo 2010-2013.

Los tres principales usos de Internet son: obtener información de carácter general (así lo declaró el 72.0% de los cibernautas); actividades de comunicación como recibir o enviar correos electrónicos (58.2%), y actividades de entretenimiento (37.1%).

Las sociedades modernas se caracterizan por un amplio uso de las Tecnologías de la Información y las Comunicaciones (en adelante TIC) en casi todos los ámbitos del quehacer humano, distinguiendo a los individuos y sus organizaciones que manejan estas herramientas tecnológicas de carácter global para ver, entender y participar, con formas innovadoras, en el mundo que nos rodea, impulsando cambios sociales y oportunidades de crecimiento.

---

<sup>(6)</sup> WALTON, Dominique, *¿Internet y después que?*, España, Barcelona., Ed., Gedisa, 2000, p. 95.

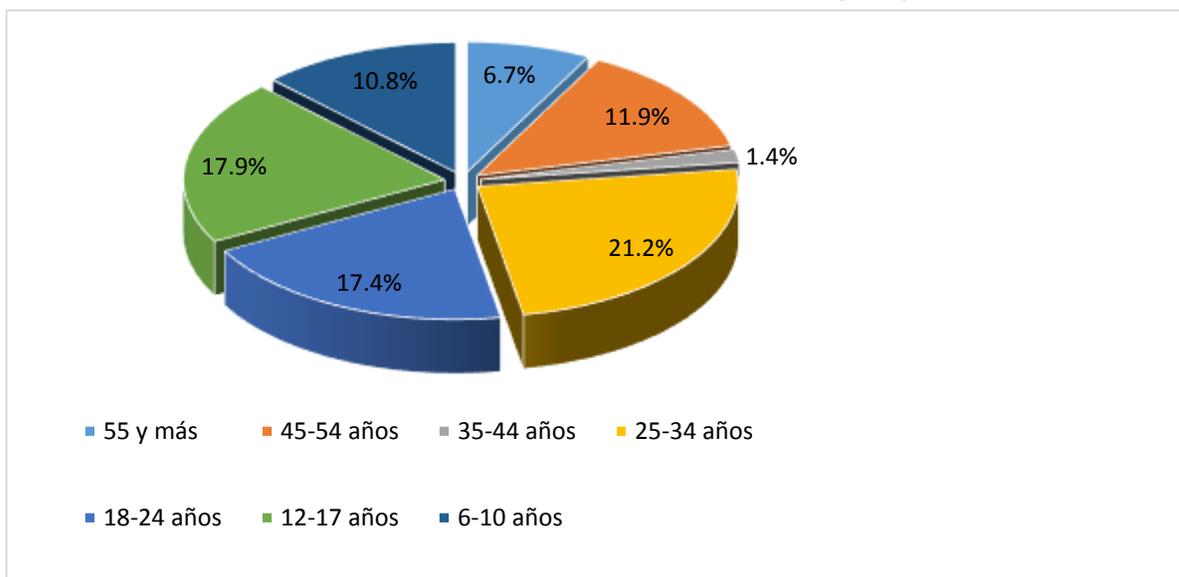
<sup>(7)</sup> *Íbid*, nota a pie (6).

Durante la Cumbre Mundial sobre la Sociedad de la Información celebrada en Túnez en 2005, se hizo un llamado a la Asamblea General de las Naciones Unidas para declarar el 17 de mayo como el Día Mundial de la Sociedad de la Información, a partir del cual surge el Día Mundial de Internet.

Por lo anterior, el Instituto Nacional de Estadística y Geografía (más adelante INEGI) presenta un panorama general del Distrito Federal, sobre el acceso a Internet en los hogares y de su uso por los individuos, con base en los resultados de la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (en adelante ENDUTIH, 2013).

El 67.3% de los cibernautas del Distrito Federal tiene menos de 35 años, lo que significa que los jóvenes son quienes más uso hacen de la tecnología, y también los primeros en adoptarlas. Tal es el caso de los niños de 6 a 11 años y de 12 a 17 que representan 10.8% y 17.9%, respectivamente, del total de usuarios de Internet.

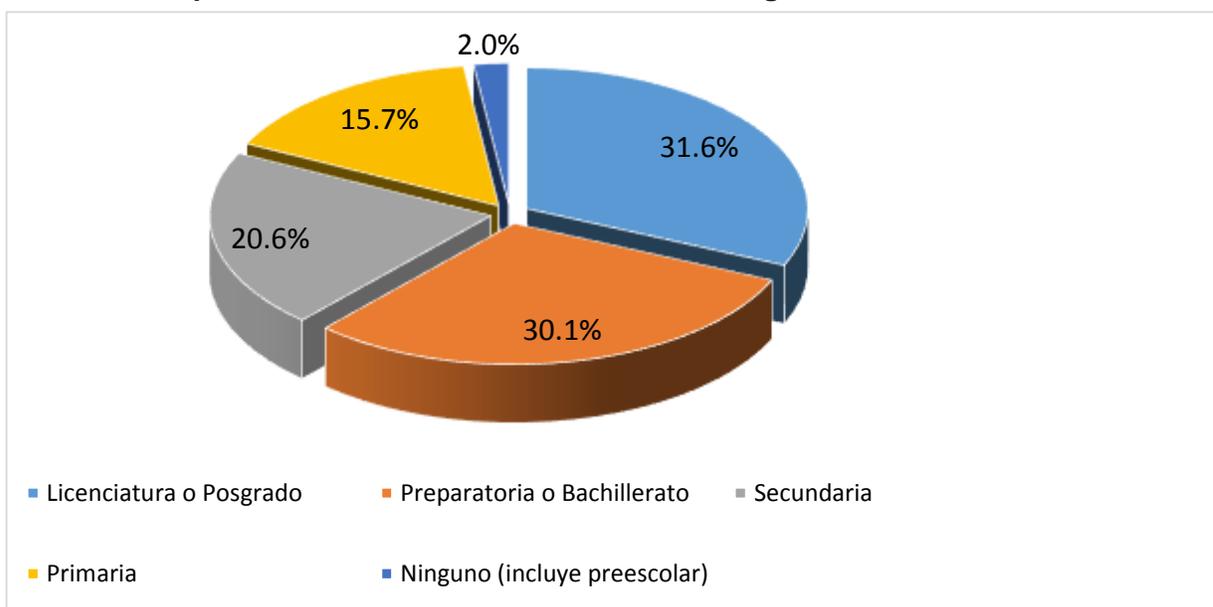
**Distribución porcentual de los usuarios de Internet según grupos de edad**



(F1) Fuente: INEGI. Encuesta sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares (ENDUTIH), 2013.

De acuerdo con los resultados de la ENDUTIH 2013, casi una tercera parte de los usuarios de Internet cuenta con algún grado en estudios de licenciatura o posgrado, esto es, 31.6%, le siguen aquellos con preparatoria o bachillerato (30.1%), mientras que 20.6% tienen algún grado en secundaria y 15.7% en primaria.

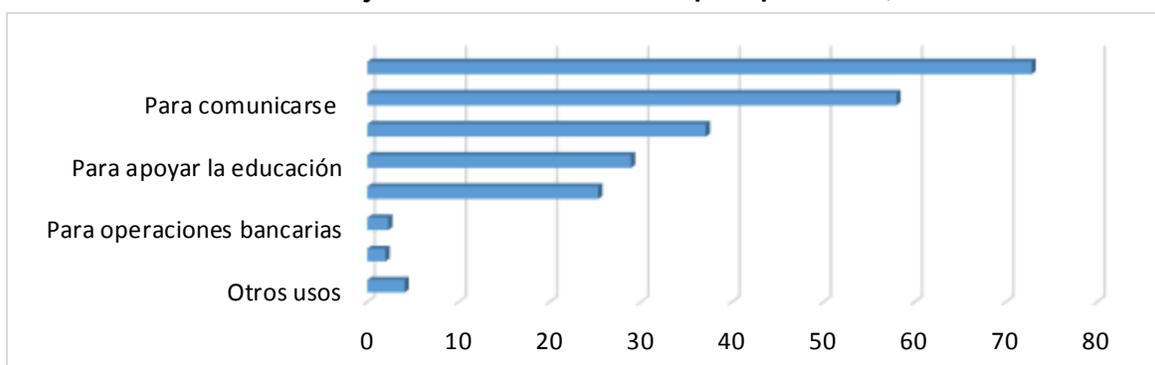
### Distribución porcentual de los usuarios de Internet según nivel de escolaridad, 2013



(F2) Fuente: INEGI. Encuesta sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares (ENDUTIH), 2013

Entre las principales actividades realizadas en Internet, la más recurrente está vinculada a la búsqueda de información (72.0%), seguida del uso como un medio de comunicación (58.2%), entretenimiento (37.1%), apoyo a la educación (28.9%) y acceso a redes sociales (25.3%).

### Porcentaje de usuarios de Internet por tipo de uso, 2013



(F3) Fuente: INEGI. Encuesta sobre Disponibilidad y Uso de las Tecnologías de la Información en los Hogares (ENDUTIH), 2013.

Así, los avances en materia de telecomunicaciones han obligado a aumentar la capacidad de los ordenadores, lo que ha permitido el desarrollo de nuevas vías de

(F2) Diseño Diana Márquez Cisneros

(F3) Diseño Diana Márquez Cisneros

negociación (formas de vender bienes y servicios), y a la par han puesto de manifiesto **las debilidades y falta de seguridad de que son objeto**, realizando la necesidad de acciones que garanticen y regulen las relaciones jurídicas que se derivan de su uso.

Adicionalmente a lo anterior, se debe de considerar el carácter transnacional de Internet (multitud de servidores dispersos por todo el mundo), ya que los problemas de jurisdicción y competencia judicial dificultan el control y aplicación de gran parte de los derechos mínimos <sup>(8)</sup> que pretenden, de algún modo, regular los contenidos o el flujo de datos a través de la red. Lo cierto es que gracias a los nuevos avances tecnológicos, estamos asistiendo a una "*desmaterialización de los actos jurídicos*" bien en **lato sensu** o en **stricto sensu**, ello sin importar donde se encuentran los objetos o los sujetos de la relación jurídica. Lo que le interesa al usuario es llegar a ellos, obtenerlos de la forma más rápida, eficiente y económica posible; lo que nos lleva a afirmar que la computadora y demás medios de telecomunicación han cambiado las nociones de tiempo, espacio, distancia, fronteras y sin duda, de soberanía; así el mundo ya no es lo que era hace unos años, la "Era Digital" lo ha cambiado para siempre, y es el Derecho quien debe regular el sano desarrollo de esta evolución. Lo que es más, hoy en día por medio de una computadora se puede realizar una llamada telefónica, situaciones que con la tecnología de hace años era impensable. Ello nos lleva al concepto de las TIC's, o Tecnologías de Información <sup>(9)</sup>. En la actualidad, el gran desarrollo y empleo de las TIC's, permite identificar a todos aquellos nacidos en esta época como "Nativos Digitales", los cuales actualmente al no haber interactuado con un mundo ausente a las TIC's, las emplean en todas sus actividades: estudiar, investigar, comprar, divertirse, socializarse e incluso enamorarse. Lo que no sucede con los "Inmigrantes Digitales", quienes están agrupados todos aquellos nacidos antes de los 90's <sup>(10)</sup>.

## 1.2. La sociedad de la información.

Hasta aquí se realizó un análisis un tanto descriptivo de las ventajas y problemas que el uso de la tecnología ha traído aparejado; sin embargo resulta conveniente hacer por un momento una reflexión de cómo es que la sociedad ha llegado hasta dónde está y cuál es el

---

<sup>(8)</sup> Debemos entender por derechos mínimos, aquellas garantías que deben tenerse en cuanto al crear una ley destinada a los usuarios de Internet, como pueden ser: el derecho a la seguridad, la libertad de expresión o el derecho a la intimidad.

<sup>(9)</sup> ESPINAR Ruiz, Eva; LÓPEZ Fernández, Cristina, **Jóvenes y adolescentes ante las nuevas tecnologías: percepción de riesgos**, Athenea Digital. Revista de Pensamiento e Investigación Social. Núm. 16 (otoño 2009) ISSN 1578-8946, p.1-20.

<sup>(10)</sup> *Ibid*, p. 25.

papel que en ese desarrollo ha jugado la tecnología, y consecuencia de ello, dedicaré el presente apartado a puntualizar algunos episodios históricos que a mi juicio resultan relevantes para comprender a la sociedad de la información en la que estamos inmersos.

### **1.2.1. El Siglo XIX y la Revolución Industrial.**

Al inicio del Siglo XIX, la civilización tenía un nuevo rostro y es que a partir de la Revolución Industrial se presentaron dos grandes fenómenos demográficos, el más notorio de ellos, la urbanización, la cual sobrevino tras el invento de la máquina de vapor, surgiendo de esa manera los primeros grandes asentamientos.

El segundo gran fenómeno demográfico se caracterizó por la concentración de cada vez más gente en las ciudades; sin embargo, más allá del movimiento campo-ciudad, estos comportamientos se tradujeron en el drástico aumento de la población que sobrevino durante el siglo posterior a la Revolución Industrial: de 790 millones de habitantes que se considera que había en 1750 pasaron a 1,260 millones en 1850 y para 1900, había ya 1,650 millones de personas en la Tierra <sup>(11)</sup> lo que revela sin duda que la humanidad había modificado su manera de comprender al mundo y se daba cuenta de la influencia que podía ejercer sobre él.

Los inventos tecnológicos y los descubrimientos científicos que sucedieron como consecuencia de la Revolución Industrial, fueron de la mano con los cambios en el pensamiento, así, la edad contemporánea que comenzó con la Revolución Francesa en 1789, fue el principio de las reformas político-sociales que se dieron en occidente, por ejemplo en Europa el poder le fue quitado a la burguesía y a la aristocracia le fueron negados los privilegios de que habían gozado siempre. Se proclamaron los Derechos Universales del Hombre y en toda América se sucedieron una serie de movimientos independentistas <sup>(12)</sup>.

### **1.2.2. El Siglo XX, inicio de toda una era de evolución científica y tecnológica.**

A principios del Siglo XX una serie de grandes adelantos tecnológicos, trajo como consecuencia que las barreras políticas y culturales comenzaran a caer, en 1908, Henry

---

<sup>(11)</sup> INEGI, *Historia de la informática*, [En línea]: Ciberhábitat Ciudad de la Información. Diciembre 2000, Actualizado Agosto 2001. <[http://ciberhabitat.gob.mx/museo/historia/texto/texto\\_sigxx.htm](http://ciberhabitat.gob.mx/museo/historia/texto/texto_sigxx.htm)> [Consulta: 18. feb. 2015].

<sup>(12)</sup> Otro ejemplo del cambio de pensamiento consecuencia de la Revolución Industrial fueron los movimientos imperialistas que extendieron sus brazos al sur de Asia y algunos países africanos; que provocarían una rivalidad que años más tarde desembocaría en la Primera Guerra Mundial; mientras que en otros países se sucedieron conflictos sociales internos, como es el caso de las revoluciones mexicana y rusa.

Ford un brillante Empresario norteamericano popularizó el automóvil y sólo tres años más tarde Charles Franklin Kettering desarrolló el motor eléctrico de arranque automático, con lo que el invento de Ford resultó más seguro y práctico.

Las comunicaciones también se revolucionaron, con la fundación de las primeras aerolíneas comerciales, que permitían arribar en poco tiempo a ciudades distantes siempre y cuando estuvieran en el mismo continente.

En 1915, el científico alemán Albert Einstein desarrolla su *Teoría de la Relatividad General* y con ello revoluciona los conceptos de espacio y tiempo, que fueron necesarios para el desarrollo de la llamada realidad virtual.

Para este momento, la humanidad ya transmitía los primeros mensajes a larga distancias como consecuencia del uso del telégrafo, y posteriormente del teléfono. Poco después entran a escena los medios masivos de comunicación, pues gracias a la radio, que ya había empezado a circular desde el siglo anterior, se da la posibilidad de ejercer la comunicación en tiempo real de un lugar a otro.

En 1925, el inventor escocés John Baird, usando una célula fotoeléctrica, transmitió imágenes en movimiento a un receptor lejano; con lo que se había inventado otro medio que no tardaría en convertirse en una parte esencial de los hogares ciudadanos: la televisión<sup>(13)</sup> la cual tres años después (1928), se transmitía por primera vez una señal experimental que cruzó el océano Atlántico y a partir de ese momento, las modificaciones y perfeccionamientos de la televisión se sucedieron rápidamente hasta lograr que las imágenes pudieran ser enviadas a una mayor distancia, ya fuese por ondas hertzianas, cables eléctricos especiales capaces de abarcar una amplia gama de señales o a través de un satélite.

### **1.2.3. La era digital: a la luz de una evolución e influencia en la vida cotidiana del Hombre.**

Durante el primer cuarto del Siglo XX la vida en hogares y sitios de trabajo comenzó a iluminarse gracias a la energía eléctrica: el foco, invento de Tomás Alva-Edison, llenó de luz las calles; un ejército de aparatos electrodomésticos comenzó entonces la toma de los

---

<sup>(13)</sup> *Íbidem*, nota a pie (11).

hogares, mientras que la radio musicalizó las vidas urbanas y el teléfono se consolidó como un actor protagónico de la vida moderna.

Poco después surge la primera computadora automática diseñada para procesar en grandes cantidades información, y su construcción se debe a la necesidad de generar el último censo estadounidense de población del Siglo XIX, cuando ese país ocupaba el primer puesto en la producción industrial mundial, y fue un inmigrante alemán nacionalizado estadounidense y graduado en la Universidad de Columbia, Herman Hollerith, quien inventó una computadora a la cual bautizó como “*Máquina Automática Perforadora de Tarjetas*”<sup>(14)</sup>, que daría pie al surgimiento de una industria: la de las computadoras, pero también, como ocurre con la creación de todo invento, generaría nuevas posibilidades.

Algunas fuentes indican que gracias al invento de la máquina perforadora, el costo del procesamiento de datos del Censo de 1890 fue 98% más caro que el del anterior, sin embargo, los resultados no sólo se obtuvieron mucho tiempo antes, sino que resultaron más completos<sup>(15)</sup>, por lo que se puede afirmar que el desarrollo de las nuevas tecnologías es la solución más eficaz a necesidades previas, pero a la vez, el principio de nuevas necesidades.

Durante los primeros años del Siglo XX Hollerith viajó por América y Europa para hacer promoción a su invento, el cual fue perfeccionando continuamente, en especial en cuanto a velocidad, todo ello, con el mismo objetivo: guardar, organizar, clasificar y procesar velozmente grandes cantidades de información y aunque en un principio el objetivo era meramente técnico, después se hizo más simple: *Hacer negocios*; es así como Hollerith comenzó a desarrollar tecnología a partir de acertadas decisiones comerciales y en menos de 20 años, patentó más de 30 inventos en América y Europa los cuales comenzaron a automatizar la vida en oficinas, tanto públicas como de grandes Empresas privadas.<sup>(16)</sup>

En 1911, a partir de la fusión de *TBM* con otras dos Empresas — *International Time Recording* y *Dayton Scale Co.*—, se creó la *Computing Tabulating-Recording Company* y finalmente, la cual en 1924 cambió su nombre por el de *International Business Machines* o *IBM*, la cual se convirtió en la mayor proveedora de equipamiento de contabilidad, y más

---

<sup>(14)</sup> CARRASCO-RODRÍGUEZ, Alberto, *et al.*, *Historia de la informática y metodología científica* [En línea] Biografías de Personajes Científicos e Informáticos < <http://usuarios.lycos.es/hv1102/hollerith.html> > [Consulta 18. feb. 2015].

<sup>(15)</sup> INEGI, nota a pie (11).

<sup>(16)</sup> *Ídem.*

tarde, de computadoras. Bajo este esquema, uno de los resultados de la introducción del paradigma de la información electrónica a mediados de la década de los años setenta fue la aceleración y masificación de la información, y en quince años, las microcomputadoras pasaron de ser máquinas con 4Kb <sup>(17)</sup> de memoria, y a las que se les daba órdenes a través de un lenguaje de programación denominado “BASIC”, a tener una memoria de 16Mb en 1989. En 1982 *Apple* introdujo en el mercado la computadora personal y ya para 1998, las computadoras personales funcionan con almacenamiento de 7Gb y 64Mb de memoria RAM<sup>(18)</sup>, utilizan programas de alta complejidad que han reemplazado la instrucción directa, y han pasado a ser dirigidas por flechas y doble clic o *User friendly* <sup>(19)</sup>.

En la sociedad moderna se ha creado una dependencia de la tecnología, lo cual se puede ver en las universidades, bibliotecas, tiendas, fábricas y hasta en los hogares, por lo que podemos decir que la “**Revolución Tecnológica**” ha impactado en todo lo que concierne a la vida moderna. Desde el modo en que usamos el dinero a través de cajeros automáticos y la necesidad de estaciones de servicio, máquinas registradoras así como la aparición de relojes que hablan, camiones que tocan música cuando retroceden, aparatos de sonido y discos compactos, pantallas de automóviles que indican cuando distintas partes del automóvil no están siendo tratadas correctamente, teléfonos inalámbricos, teléfonos de tono, y todo lo demás que es digital.

Sería impensable el mundo como lo conocemos a principios del Siglo XXI, sin los avances de la ciencia y la tecnología; éstos, han tenido resultados muy positivos para la recuperación de los países desarrollados, porque han permitido ahorrar mano de obra, materias primas y energía, además de haber acelerado el ritmo de innovación; sin embargo, algunos no han sido tan buenos, puesto que el ahorro de la mano de obra ha generado un desempleo irreversible, dado que el número de personas requeridas para producir una

---

<sup>(17)</sup> La unidad de medición de la capacidad de memoria de los equipos informáticos está dada en Bits. Un bit representa un dato o un carácter almacenando al interior de la computadora, sin embargo al ser los bits, unidades tan pequeñas de medición en comparación con la cantidad de información que puede llegar a almacenarse en un ordenador, normalmente la capacidad de memoria se expresa en Bites un múltiplo de la unidad que contiene aproximadamente 1024 bits y no es el único múltiplo de esta unidad que existe pues también tenemos al Kilo Bite (Kb) el Mega bite (Mb) y el Giga Bite (Gb).

<sup>(18)</sup> Del Inglés Random Acces Memory, que en términos más o menos técnicos significa Memoria de solo acceso; es un espacio de memoria volátil del ordenador que se utiliza sólo para almacenar las operaciones que está ejecutando la computadora en el momento, esta memoria determina el número de operaciones por segundo que es capaz de realizar una computadora, por lo que entre mayor sea el tamaño del RAM, mayor será el número de operaciones que será capaz de realizar.

<sup>(19)</sup> *User friendly* es el nombre en inglés de un sistema de comunicación con las computadoras que hace que la interacción máquina- usuario sea simple. Hoy en día la mayoría de los programas usan esta directriz, y es lo que ha hecho tan popular a los sistemas operativos como Windows, que está basado en “ventanas” y que obtiene el máximo provecho del uso del Mouse.

cantidad igual de bienes es menor hoy que hace diez años, y la relación entre países productores de materias primas y productores de manufacturas se ha deteriorado aún más a causa del ahorro que la nueva tecnología permite, ello debido a la asistencia que han provisto para producir sustitutos manufacturados por el hombre y a la reducción del tamaño de los productos finales a veces hasta casi desmaterializarse.

En otra dimensión, con la aceleración del flujo de la información también podemos entablar conversaciones por el correo electrónico en cualquier parte del mundo desde la comodidad de nuestros hogares; hoy por hoy, podemos estar en todas partes. En tan solo doscientos años el mundo ha cambiado radicalmente, gracias a la tecnología, quienes vivimos en el presente siglo podemos contar con medios y herramientas que nunca pensamos, lo que trae aparejada la responsabilidad de superar los problemas que con el uso de los adelantos tecnológicos se han generado o pudieran generarse.

### **1.3. Las herramientas de la Internet: un desafío para la práctica jurídica.**

El número de servicios que operan en la Red, empiezan ahora a incrementarse de una manera casi exponencial, en esta época operan bancos en la red como lo es el *First Virtual* <sup>(20)</sup>, una radio comercial de difusión exclusiva en Internet llamada *Radio HK* que poco después se convirtió en *Real Audio*, uno de los proveedores de servicios multimedia más populares de la Red; en nuestros días los Gobiernos de todo el mundo se conectan a la red, y el registro de los dominios deja de ser gratuito para pagarse una cuota anual de cincuenta dólares. Actualmente se desarrollan nuevos motores de búsqueda (*search engines*) que añaden búsquedas inteligentes en varios idiomas.

En ese tenor, el lenguaje *Java* <sup>(21)</sup> empieza a popularizarse, se desarrollan tecnologías como entornos virtuales (*VRML*) o el teléfono por Internet, que permite llamar por teléfono a todo el mundo al precio de una llamada local. Todos estos adelantos, tienen una gran relevancia en las relaciones comerciales, sea para comprar productos o para obtener servicios a través de Internet, además de que gracias a este medio, también se

---

<sup>(20)</sup> El First Virtual Bank, es el proyecto conjunto con el banco First USA que permite a los compradores de la Internet o World Wide Web abrir cuentas centrales utilizando tarjetas de crédito, de ésta forma los compradores pueden usar sus números cuenta para hacer compras en cualquiera de un número de comercios participantes. Vid, Hutchinson Encyclopedia, [En línea] Dictionary. Computers [USA] <<http://www.tiscali.co.uk/reference/dictionaries/computers/data/m0051242.html>> [Consulta: 21. feb. 2015].

<sup>(21)</sup> JAVA es un Lenguaje de programación orientado a objetos muy parecido al diverso C++, es comúnmente utilizado por programadores y diseñadores de la Red para la telecarga o ejecución a distancia de programas en la computadora del usuario del sitio y fue desarrollado por Sun Microsystems.

pueden ver cientos de canales de televisión y escuchar estaciones de radio de todo el mundo en tiempo real.

Los bancos se asientan en la Red y la gente empieza a confiar en la seguridad que ofrecen los “servidores seguros” dejando su miedo inicial a las transacciones por Internet. Aparecen los primeros virus de *HTML* <sup>(22)</sup> que son virus de macro incrustados en documentos de Word, que se transmiten por correo electrónico como *attachment* <sup>(23)</sup> y se ejecutan en las máquinas sin protección contra virus de macro.

Al margen de los peligros tecnológicos, otro ejemplo lo es la tecnología de telefonía móvil y la de Internet, que al unirse, permiten acceder desde los teléfonos móviles a la Red de redes, y aunque si bien es cierto que dispositivos inalámbricos ya accedían a la Red, es con la definición del conjunto de protocolos *WAP (Wireless Application Protocol)* <sup>(24)</sup> cuando los dispositivos inalámbricos y fundamentalmente los teléfonos móviles, se conectan a Internet, surgiendo entonces el *WAP Forum*, que hoy agrupa al 90% de los fabricantes de teléfonos móviles y cubre unos 100 millones de teléfonos en todo el mundo.

Consecuencia de todos estos cambios, el Derecho no puede ni debe quedarse inmutable ante esta realidad, empero, poco a poco se va mudando de las bibliotecas, de las oficinas de los abogados, de los libros, de los juzgados, del mundo de los contratos escritos, así como de los expedientes donde eran archivados, quedando esta información ya solo disponible en las pantallas de las computadoras; así consultamos el saldo de nuestra cuenta bancaria y hasta el estado procesal de nuestros juicios <sup>(25)</sup>.

Es un desafío de la tradicional forma de ejercer la profesión y sus conceptos hacia un ambiente donde el valor de la información crece, en un mundo de espacios más flexibles, de nuevas relaciones, generando un apasionante desafío de adaptación a los tiempos con el riesgo *darwiniano* de evolucionar o morir. En ese sentido, y para comprender un poco mejor

---

<sup>(22)</sup> *HTML* son las siglas en inglés que sirven para referirse a *Hiper-Text Markup Language* que aunque no se considera realmente un lenguaje de programación, la mayoría de los documentos en el Internet se escriben utilizando este sistema de etiquetas, originalmente se pensó que era un sistema seguro de distribución a través de la Red, debido a que solo podía indicar a los ordenadores la forma en la que se debía de representar un determinado texto, sin embargo hoy en día ya es posible difundir un virus informático haciendo uso de este lenguaje

<sup>(23)</sup> *Attachment*, es el término anglosajón que se emplea para referirse a los archivos que se adjuntan a un mensaje de correo electrónico, en nuestro país es común usar esta expresión o sustituirla por la frase “archivo adjunto”.

<sup>(24)</sup> *Wireless Application Protocol*, del Inglés Protocolo de Aplicación Inalámbrica.

<sup>(25)</sup> Basta referirnos a la página Web de la Suprema Corte de Justicia de la Nación ([www.scjn.gob.mx](http://www.scjn.gob.mx)), para percatarnos que es posible consultar en línea el listado aprobado tanto de los Juzgados de Distrito, como de los Tribunales Colegiados de Circuito, y no solo del circuito judicial en el que nos encontramos, sino de todo el país.

el problema técnico-jurídico al que nos enfrentamos como juristas, dedicaré algunas líneas sobre los tres servicios básicos de los que está constituido el Internet y que son a los que la mayoría de los usuarios tenemos acceso: a) El correo electrónico, b) Los grupos de noticias y c) Las máquinas de búsqueda, que en los siguientes títulos de detallan.

### 1.3.1. El correo electrónico.

El correo electrónico es una especie de apartado postal, solo que en vez de existir en el mundo físico, éste existe en el mundo virtual, es una porción de espacio designada para nuestro uso dentro de una computadora de gran capacidad a la que se denomina servidor. El correo electrónico o **E-mail**, funciona gracias a la creación de direcciones de correo electrónico que se conforman de tres partes: un nombre de usuario o **login**, seguido del carácter “@” que indica que se trata de una dirección de correo electrónico, seguidos éstos de un dominio <sup>(26)</sup> que puede ser internacional o nacional (local).

A este respecto Prenafeta <sup>(27)</sup> señala en términos generales que la Agencia Española de Protección Datos distingue entre dos clases de correos, por un lado están los que poseen datos de carácter personal que son aquellas direcciones de correo electrónico que contienen información acerca del titular, como el nombre o apellidos (o sus iniciales), la entidad en la que trabaja (dominio de segundo nivel) y el país en el que lleva a cabo su actividad (dominio de primer nivel); y por otro lado tenemos a aquellas direcciones de correo que no muestran directamente datos relacionados con el titular de la cuenta, sino una denominación abstracta o un conjunto de caracteres alfanuméricos sin significado alguno.

El segundo de los tipos de direcciones de correo electrónico, es quizás el que suscita el mayor número de problemas, como pueden ser los derivados de la falta de identificación de la persona con la que se interactúa, o el problema de la ubicación de un proveedor que se encuentra en otro país y con el que sólo se ha tenido contacto vía electrónica.

Aunque también en las direcciones que no muestran información personal se puede llegar a identificar al titular de la cuenta, esto sólo es posible mediante una consulta al servidor que gestione el dominio. Por lo que se concluye que la dirección de correo

---

<sup>(26)</sup> El concepto dominio es popular entre los cibernautas, ya que hacen referencia a una parte del nombre jerárquico con que se conoce cada entidad conectada a Internet. Sintácticamente, un dominio (*domain*) de Internet se compone de una de etiquetas o nombres separados por puntos.

<sup>(27)</sup> PRENAFETA-RODRÍGUEZ, Javier, **Protección de datos de carácter personal e Internet**, [En línea]: Artículos doctrinales: Derecho Informático, agosto 2002, <<http://noticias.juridicas.com/areas/20-Derecho%20Inform%E1tico/10-Art%EDculos/200208-55561531610232111.html#foot11>> [Consulta 22. feb. 2015].

electrónico es un dato de carácter personal y que debe protegerse como parte del derecho a la privacidad. El problema surge cuando haciendo uso de este anonimato que la Red permite, se vulneran los derechos de otros usuarios, y es precisamente cuando el problema deja de ser técnico para entrar al campo de lo jurídico.

### **1.3.2. Los grupos de noticias.**

Éste es otro servicio que provee Internet, donde por medio de los foros y listas de correo (que podemos considerar formas de los grupos de noticias) el usuario puede manifestar opiniones, preferencias o inquietudes, ya sea a través de la Red o del correo electrónico. Dadas las facilidades de la informática, estos datos pueden almacenarse durante varios años en los servidores de los proveedores, por lo que un rastreo permitiría recopilar, sin que el afectado fuera consciente, una cantidad de información suficiente para el establecimiento de su perfil (nivel socioeconómico, preferencias y disgustos, así como amistades).

La Agencia Española de Protección de Datos y el Consejo de Europa, el *International Working Group on Data Protection in Telecommunications*, así como el Grupo de Trabajo sobre Protección de Datos de la Unión Europea (en adelante UE), aconsejan ser conscientes de que las opiniones vertidas en dichos foros y listas son públicas y pueden ser malinterpretadas, siendo una excelente fuente para el surgimiento de responsabilidades, por lo cual, se anima a los usuarios a utilizar todos los mecanismos posibles para preservar el anonimato en la red, anonimato que también constituye un problema jurídico.

### **1.3.3. Máquinas de búsqueda.**

Son el tercero y quizás más popular servicio que ofrece la Internet, y siguiendo a Prenafeta <sup>(28)</sup>, son poderosas computadoras que se encargan de investigar por nosotros una gran cantidad de páginas Web, para encontrar en ellas alguna palabra o palabras clave que coincida con los criterios de búsqueda que para tal efecto hemos introducido, en ese sentido, nuestro autor distingue tres tipos de herramientas de búsqueda:

- i. **Los llamados genéricamente buscadores**, son aquellas máquinas de búsqueda que ofrecen direcciones o sitios de Internet relacionados con la búsqueda solicitada (Vg. *www.terra.es* o *www.yahoo.com*).

---

<sup>(28)</sup> *Ibíd.*

- ii. **Los motores de búsqueda**, se llama así a aquellos buscadores que por su cuenta rastrean la red y crean bases de datos documentales que pueden ser consultadas por los usuarios (Vg. *www.google.com*, *www.alltheweb.com*).
- iii. **Los agentes inteligentes o netbots**, que incorporan mecanismos que permiten el filtrado de contenidos, pueden informarnos de actualizaciones y cambios en páginas Web, aprenden de las búsquedas anteriores, no sólo de las del propio usuario, sino de las realizadas por otros con las mismas preferencias que nosotros, e incorporan todo tipo de mecanismos que, procesando el lenguaje natural, ajustan los resultados de la búsqueda al máximo, a partir, eso sí, de un conocimiento muy completo de los intereses del usuario. En materia de negocios, se suelen utilizar para buscar productos que se ajusten a un margen de precios, utilidades o preferencias del usuario, como es el caso de la tienda virtual *Amazon (www.amazon.com)* que propone junto a los libros cuyo título o contenido se ajustan a la búsqueda, otros libros de la misma temática, otros que han comprado usuarios con un interés semejante, o incluso productos de música o vídeo que estén relacionados.

Otro ejemplo de agentes inteligentes, es el *eService Center* desarrollado por la Empresa norteamericana *RightNow (www.rightnow.com)* para gestionar de forma más eficiente los servicios de atención al cliente. Su novedad es que el sistema no tiene que anticiparse a las posibles preguntas de los usuarios sino que va aprendiendo con cada consulta hecha por éstos y va clasificando las respuestas a medida que se van generando. La aplicación <sup>(29)</sup> reconoce en las consultas (por correo electrónico), ciertas palabras clave por medio de las cuales puede llegar a comprender dichas consultas, realizar estadísticas y hasta generar respuestas personalizadas utilizando plantillas.

En principio Internet agrupa un conjunto de servicios, que se vinculan a través de protocolos técnicos que le permiten intercomunicar a los usuarios entre sí; pero lo realmente sorprendente, es que toda esta cantidad de información pueda agruparse, según sostiene Dominique <sup>(30)</sup>, en cuatro grandes categorías:

---

<sup>(29)</sup> Se llama aplicación a cada uno de los programas que, una vez ejecutados, permiten trabajar con el ordenador. Son aplicaciones los procesadores de textos, hojas de cálculo, bases de datos, programas de dibujo, paquetes estadísticos, etc.

<sup>(30)</sup> DOMINIQUE..., *op. cit.*, nota a pie (6), p.100.

1. **Aplicaciones Tipo Servicios.** Comúnmente utilizadas para el intercambio de cualquier información y a veces para realizar transacciones; por ejemplo los anuncios, los horóscopos en línea, el estado del tiempo y los buscadores.
2. **Aplicaciones Tipo Ocio.** Se refiere a la gran cantidad de Juegos Interactivos que pueden ser encontrados en la Red, así como a las aplicaciones que permiten acceso a música, video y algunas otras opciones multimedia.
3. **Aplicaciones Tipo Información-Acontecimiento.** Se define así a aquella información o utilidad que normalmente es suministrada por agencias de noticias especializadas o asociaciones profesionales o culturales.
4. **Aplicaciones Tipo Información-Conocimiento.** Es aquella información puesta a disposición en bases de datos a los que se puede tener libre acceso, aunque a menudo requieran de una membresía o alguna clave de acceso.

Independientemente de la forma en la que se agrupen o clasifiquen estos servicios, el problema son los riesgos a que se exponen los usuarios promedio de estas aplicaciones, quienes no son del todo conscientes del funcionamiento de las mismas y quedan expuestos a que el sector privado, o peor aún un grupo criminal, recopile y sistematice los rastros de información que van dejándose en la red, al efecto de construir carteras de potenciales clientes u objetivos.

Otros retos a resolver por legisladores y juristas, son sin duda el tráfico de software pirata, los problemas del *Hacking* y *Cracking* <sup>(31)</sup> y de los ahora perseguidos y combatidos programas de “archivos compartidos” como el finado *Napster* o el agonizante *Kazaa*; y a ellos debemos agregar el riesgo de los contenidos ofensivos, léase pornografía, racismo, antisemitismo o sectarismo, que contaminan los caminos del ciber-espacio y al que los niños y jóvenes pueden ser expuestos casi sin darse cuenta.

---

<sup>(31)</sup> El *hacking* es un asunto de seguridad informática, representado por los **Hackers**, individuos altamente conocedores de los sistemas informáticos que se infiltran a los mismos con el objetivo de hurtar información o simplemente por el reto que representa la infiltración; en la mayoría de las ocasiones sus actividades se limitan a la protesta o las bromas pesadas, sin embargo en ocasiones pueden llegar a ocasionar serios daños a los sistemas que son víctimas de sus ataques. Por otro lado está el **Cracker**, que es una especie de **Hacker** cuya ocupación es buscar la forma de entrar en sistemas y encontrar las fallas de seguridad de los programas.

#### 1.4. El orden público digital: un necesario replanteamiento de juridicidad.

En un estudio realizado por Horacio R. Granero <sup>(32)</sup> para el Instituto de Informática Jurídica de la Universidad del Salvador acerca del impacto de las nuevas tecnologías en el Derecho, el catedrático pone de manifiesto el uso de la llamada “Alta tecnología” en la vida cotidiana (*supra*, § 1.3) establece la necesidad de un estudio jurídico serio, por lo que propone el establecimiento de un nuevo orden público económico especialmente en lo tocante a los contratos electrónicos, a través del cual se impida a las partes colocar los riesgos propios del contratante profesional sobre la parte más débil, sobre todo si ésta no cuenta con un mínimo básico de conocimientos en materia de tecnología, que le permitan comprender en lo esencial las obligaciones que asume.

En el marco del Derecho mexicano, la idea de Granero no sería considerada novedad, el Poder Constituyente Permanente no fue indolente y se ocupó de definir y recoger este concepto dentro del artículo 28 de la Constitución General de la República. En efecto, en el citado numeral se establecen los lineamientos a través de los cuales el Estado puede intervenir en la economía nacional, para el efecto de conducir el desarrollo del país. En ese sentido lo que Granero propone no es algo desconocido para el legislador mexicano, sino que por el contrario, se halla desde 1983 con rango constitucional, el deber del Estado de intervenir y ser rector de la planeación democrática del desarrollo económico tanto en áreas prioritarias como estratégicas, para el uso racional de los recursos (materiales, financieros e institucionales) con que cuenta.

Por tanto, si el artículo 28 de la Constitución Política de los Estados Unidos Mexicanos permite al estado intervenir en la planeación económica y en el combate a los monopolios, no creemos que exista algún impedimento para que también intervenga en el uso comercial de las comunicaciones, máxime si se considera que de acuerdo con el artículo 25 de la propia Constitución, están obligados a concurrir responsablemente al desarrollo económico nacional el **sector público**, el sector social y el **sector privado**.

Extremando el análisis, se ha llegado a hablar de un orden público tecnológico, para evidenciar la necesidad de una protección más adecuada del consumidor ante el advenimiento de tecnologías sofisticadas, y es que la complejidad de las prestaciones y de

---

<sup>(32)</sup> GRANERO, Horacio R., *El impacto de las nuevas tecnologías en las Empresas*, [En línea] Instituto de Informática Jurídica de la Universidad del Salvador. (El derecho y la Alta tecnología) <<http://www.ijprofesional.com.ar/index.php?idnoticia=61&return=entrevistas&Page=>> [Consulta 24. feb. 2015].

los productos que forman el objeto de los **computer contracts** <sup>(33)</sup>, hace evidentes las diferencias entre las partes.

Puede decirse entonces, que el impacto de la tecnología en la sociedad suscita diversos problemas jurídicos que no pueden ser resueltos por la normativa tradicional, verbigracia:

- a) Validez legal de los documentos transferidos electrónicamente y régimen aplicable.
- b) Régimen de la publicidad y sanciones por su uso indebido.
- c) Infracción de marcas (Vg. titularidad de los "dominios" en Internet).
- d) Régimen de venta a distancia en lo que concierne a las normas que rigen las condiciones de oferta pública en la venta de productos y servicios.
- e) Violaciones al derecho a la imagen y a la vida privada, cuestiones de seguridad, criptografía y protección de datos, responsabilidad relativa a la difusión de información o de imágenes.
- f) Imposibilidad de garantizar los derechos de propiedad intelectual de las obras publicadas en Internet.

Todas estas cuestiones generan un apasionante desafío para los juristas, y es que el Derecho ya es suficientemente complejo cuando estamos tratando con conceptos bien conocidas (documentos escritos en papel, con firma autógrafa y en base a instituciones legales bien definidas), pero el resultado del gran vacío que nos propone la alta tecnología se presenta como un borroso mundo de computadoras interconectadas, sin precedentes valederos ni experiencia suficiente para dar opiniones con un grado de certeza que por lo menos sea aceptable. Esta situación ha puesto a muchos en guardia y ha obligado a pensar en una normatividad que deba seguir ciertas pautas lógicas conformadas por nuestras actuales concepciones de la realidad, siendo cuidadosos, pero sin olvidar que el **ciberespacio** es meramente una extensión de nuestras fronteras físicas, después de todo detrás de cada terminal de computación a cargo de emitir cada comando, se halla simplemente otra persona más.

Mientras los legisladores y los tribunales luchan por mantenerse a tono con la tecnología, la precaución y el sentido común debería ser nuestros principios guía, y en esa tarea no debe estar ajena la Universidad. Una cosa es "universalidad de conocimientos" o

---

<sup>(33)</sup> Del inglés "Contratos Computacionales".

mera "informatización", para lo cual nos servimos de computadoras, y otra muy diversa es "universalidad del conocimiento" que consiste en encontrar lo verdadero y saber otorgar un sentido a lo poco o mucho que se sepa.

Así, por lo menos lo entendió la Universidad Católica Argentina "Santa María de los Buenos Aires" cuando a fines de 1997, creó dentro del ámbito de la Facultad de Derecho la Carrera de Postgrado de *Abogado Especialista en Derecho de la Alta Tecnología* <sup>(34)</sup>, cuyo título cuenta hoy con validez nacional (Res. N° 677 del Ministerio de Educación del 14 de abril de 1998), con el afán de formar abogados con capacidad para afrontar los desafíos que la tecnología origina, pero sin olvidar el fin primordial universitario que consiste en la formación de profesionales e investigadores.

### **1.5. Usos y costumbres virtuales: un acotamiento a las exigencias axiológicas y técnico-gramaticales.**

En la actualidad existe una verdadera **sociedad virtual**, que vive y evoluciona a su propio ritmo y en ocasiones pareciera que lo hace de manera independiente de la vida fuera de la red, incluso con sus propios usos y costumbres virtuales a las que me he referido de manera muy somera, solo para reforzar éste argumento en el sentido de que se necesita una rama del Derecho que se especialice en atender los problemas jurídicos derivados con la protección de datos personales en posesión de los particulares y seguridad de la información. Para ello, es menester referirse al denominado **Netiquette** (llamado también el "Protocolo y Buenas Costumbres Virtuales") que es un conjunto de normas morales que dentro de los usuarios de las redes informáticas, cada día se populariza más y que están haciendo de las comunidades de usuarios verdaderas sociedades digitales.

Gracias a una renovada cultura del lápiz y el papel, a diario se actualizan en el ciberespacio ciertas conductas para comunicarse con otras personas a través del correo electrónico, y que son las bases de una normatividad que sugiere modales correctos en donde el contacto impersonal y sin rostro ya es parte de lo cotidiano. A este conjunto de sugerencias se le denomina **Netiquette** y su objeto es humanizar lo naturalmente inhumano, tratando de imprimir rasgos de cultura a una sociedad que surge y sigue los mismos pasos que su predecesora, construyendo sus propios signos de identidad. En ese orden de ideas, existen dos principios básicos que son los ejes centrales de la **Netiquette**:

---

<sup>(34)</sup> GRANERO..., *supra*, nota a pie (32).

1. Se debe recordar que al otro lado del monitor hay otro ser humano que está pendiente de lo que se escribe.
2. Hay que tener presente que se es responsable de que la comunicación tome un mejor nivel y sea un acto agradable y eficiente, así como lo es en la vida real.

Resulta conveniente hacer aquí una pausa para preguntarnos cuál es la relevancia que tiene el vocablo de la **Nettiquette** dentro de nuestro estudio, pues bien, es de explorado Derecho que el mundo normativo no solo se limita a las normas jurídicas heteroaplicativas, sino que existen una serie de normas llamadas morales, que son reglas de conducta en las cuales frente al sujeto a quien obligan no existe otra persona autorizada para exigirle el cumplimiento de sus deberes y en consecuencia, estas normas revisten las siguientes características: unilateralidad, incoercibilidad, interioridad y autonomía con algunos matices de heteronomía.

Lo anterior viene al caso, debido a que como es sabido, las normas morales, son antecedente directo de las normas jurídicas, pues establecen líneas de pensamiento social que los legisladores deben seguir al momento de dictar las leyes. En el caso concreto, consideramos que los legisladores que deban llevar a cabo leyes en materia de uso de tecnología, tienen que recordar que detrás de cada computadora se encuentra una persona, que tiene necesidad de protección jurídica y que ésta a su vez, debe ser responsable de la manera en la que interactúa con los miembros de la comunidad, justo como lo hace en la vida real.

La criptografía es una de las herramientas necesarias para garantizar, dado el caso, la confidencialidad de la información intercambiada así como la no-manipulación de la misma entre el origen y el destino, éste método que se ha popularizado entre los usuarios de las redes computacionales para construir un refugio en contra de la invasión a la privacidad de los usuarios, debido a que un E-mail puede ser rastreado automática y masivamente para detectar, por ejemplo, palabras clave utilizadas en las actividades criminales y en la subversión política, lo cual sin lugar a dudas atenta en contra de las garantías más elementales de los individuos <sup>(35)</sup>, circunstancia por la cual se debe tener la cultura de que

---

<sup>(35)</sup> *Cfr.*, MALVIDO..., *op. cit.*, nota a pie (1), p. 26, donde sostiene que algunos especialistas de la encriptación como Phil ZIMMERMANN inventor del sistema **Pretty Good Security** (Muy Buena Seguridad) propugnan a favor de considerar el derecho a la encriptación como una extensión del derecho a la privacidad, como una forma de “mantener la trinchera” en contra de la invasión de la intimidad, que los gobiernos de todo el mundo se están permitiendo.

las autoridades no deben violar la intimidad de los gobernados y fomentar el uso de la tecnología de encriptación.

Curiosamente fue Steve Russell, un juez retirado y profesor de justicia criminal de la Universidad de Texas el primero en violar la nueva ley y dirigió a los legisladores que elaboraron el proyecto, un escrito en el que puede leerse: “...patéticos... han vendido La Primera Enmienda, sus derechos heredados y los de sus hijos...”<sup>(36)</sup>. en ese mismo sentido Malvido<sup>(37)</sup> expresa: “... la nueva ley no solo desató protestas sino que fue el elemento detonante para que terminase de gestarse una nueva sociedad civil planetaria, una Comunidad Virtual...”, la cual el 8 de febrero de 1996 publicó en Internet su “Declaración de Independencia del Ciberespacio”, firmada en Davos, Suiza y redactada por John Perry Barlow, miembro de la *Electronic Frontier Foundation* (Fundación Frontera Electrónica) que a la letra contiene:

*“Gobiernos del mundo industrial, desgastados gigantes de carne y hierro, vengo del ciberespacio, el nuevo hogar de la mente. En nombre del futuro y del pasado, les pido que nos dejen en paz. No son bienvenidos entre nosotros. No tienen ninguna supremacía donde nos reunimos.*

*Los gobiernos derivan su justo poder del consentimiento de los gobernados. Ustedes no han solicitado ni recibido el nuestro...*

...

*No tenemos ningún gobierno electo ni parece factible que lo tengamos...”*<sup>(38)</sup>.

Como vemos, ésta es la nueva sociedad a la que va dirigido el Derecho de las Nuevas Tecnologías, una comunidad independiente, que aunque pudiera decirse pretende escapar del mundo material, necesariamente permanece a él y requiere del reconocimiento de su existencia y diferencia, para recibir un trato justo socialmente hablando, será entonces necesario salir del vacío jurídico actual, puesto que una Red sin normatividad específica es una red destrozada por los peores virus: La desigualdad y la manipulación<sup>(39)</sup>.

Queda entonces claro que existe una comunidad virtual que posee sus propias reglas que vive y crece en un mundo virtual, realizando la misma clase de interacción humana que se lleva a cabo en el mundo real, que se relaciona, intercambia información, compra, vende,

---

<sup>(36)</sup> *Íbidem*, p. 204

<sup>(37)</sup> *Ídem*.

<sup>(38)</sup> *Ídem*.

<sup>(39)</sup> WALTON..., *supra*, nota a pie (6), p. 112.

etcétera. Por ello, es vital que las organizaciones que interactúan en este mundo virtual contemplen los nuevos retos que implica el estar siempre conectados.

Uno de estos retos es la seguridad de la información que compartimos y la protección de los datos personales que utilizamos debido a la preocupación creciente del mal uso que se le pueda dar y la posible explotación de esta información, situación que podría derivar en molestias o riesgos en la integridad de las personas.

Debido a lo anterior, es importante que las Empresas cuenten con información específica y tengan acceso a la transferencia de conocimiento por parte de expertos en la materia, sobre los requisitos que deberán cumplir como son: cumplimiento de principios, creación e implementación de un documento de seguridad, además de contar con procedimientos adecuados para publicar el aviso de privacidad, para obtener el consentimiento de los titulares y para atender la solicitudes de derechos de acceso, rectificación, cancelación y oposición (en adelante Derechos ARCO), así como en general conocimiento sobre los beneficios que se obtienen al dar un tratamiento adecuado a los datos personales, cumpliendo así con la regulación en la materia. Esta necesidad de difusión para llegar a las Empresas, será cubierta mediante mi propuesta de incluir en la currícula de la Especialidad en Derecho Empresarial orientada a sensibilizar sobre la importancia del cumplimiento con la Ley Federal de Protección de Datos Personales en Posesión de Particulares y su Reglamento, y de los beneficios que dicho cumplimiento conlleva.

## **I. Casos Particulares**

Los datos personales registrados en las bases de datos son altamente valiosos, se trata de aspectos que definen a la persona: nombre, domicilio, nacionalidad, educación, historial clínico, familia, historial crediticio, ideología, afiliación política, edad, antecedentes penales, religión, origen racial, preferencias sexuales, estado civil, etcétera. Si toda esta información circula sin ninguna restricción, con incumplimiento a las normas, leyes o tratados existentes, el cruce de información de las bases de datos puede crear perfiles completos que ponen en peligro la seguridad de las personas: podrían ser víctimas de secuestro, fraude, recibir ofertas de inversión que no solicitaron, ser víctimas de discriminación o chantaje, se les pueden negar ciertos servicios por su historial crediticio, recibir propaganda o publicidad no solicitada de acuerdo con sus hábitos de consumo, etcétera.

Es innegable que la información es una herramienta básica y necesaria para el desarrollo de toda actividad, tanto del sector público como privado, sin distinción alguna. En este capítulo se presenta un breve análisis del uso de la información que realizan diferentes sectores en nuestro país, con puntos de oportunidad y debilidades que hasta el momento ofrece la legislación y políticas públicas para su protección.

### **1.5.1. Sociedad de Información Crediticia**

La Ley Federal de Protección de Datos Personales en Posesión de Particulares, tiene por objeto proteger los datos personales y su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. La ley en comento, tiene como finalidad regular a los sujetos particulares que sean personas físicas o morales de carácter privado, con excepción de:

- Aquellas personas que lleven a cabo la recolección de datos personales para uso exclusivamente personal, y sin fines de divulgación o utilización comercial; y
- A las Sociedades de Información Crediticia.

En relación a la última excepción, cabe señalar que este tipo de entidades, denominadas Sociedades de Información Crediticia (en adelante SIC), son organizaciones que proporcionan servicios de recopilación, manejo y entrega o envío de información relativa al historial crediticio de personas físicas y morales, es decir, a los Burós de Crédito, los cuales son instituciones financieras, autorizadas por la Secretaría de Hacienda y Crédito Público (en adelante SHCP), previa opinión del Banco de México y de la Comisión Nacional de Bancaria y de Valores (en adelante CNBV).

El objetivo principal para regular a las Sociedades de Información Crediticia es proteger los derechos de los deudores respecto a su historial de crédito. Existe un sinnúmero de bases de datos que contienen información de personas que en alguna ocasión han solicitado y recibido una tarjeta de crédito comercial o bancaria, algún préstamo o servicio. Las Sociedades de Información Crediticia o Burós de Crédito estandarizan esta información y la venden a los acreedores o Empresas comerciales como un reporte de crédito. Dichos reportes sirven como referencia a las entidades financieras para determinar si las personas son sujetos de crédito o no y que les aprueben o rechacen sus solicitudes.

Las SIC reúnen información sobre el historial de crédito de las personas, tanto de entidades financieras (Bancos, Sofoles, etcétera), como de Empresas comerciales (tiendas departamentales, Empresas de financiamiento de automóviles, Empresas de telefonía celular, etcétera). Es decir, las SIC o burós crediticios, son bases de datos que administran o guardan el historial de crédito de las personas, esto es, que en dichas bases de datos se lleva un control de los adeudos (cartera vencida) que adquiera la persona contra quien haya solicitado el crédito ya sea ante algún Banco, tienda departamental, etcétera.

El principal objetivo de las SIC es proporcionar a las Empresas información sobre el historial crediticio de las personas, con la finalidad de que dicha información ayude a conocer, mediante esta base de datos el comportamiento de pago de las Empresas y personas físicas, lo cual contribuye a minimizar el riesgo crediticio.

Esto es, que las SIC tienen la finalidad de proporcionar un listado mediante el cual, cualquier proveedor de bienes y servicios puede obtener información, sobre el historial de crédito de los posibles prospectos a clientes, que busquen recibir algún tipo de financiamiento.

El Banco de México emite las Reglas Generales a las que Deberán Sujetarse las Operaciones y Actividades de las Sociedades de Información Crediticia <sup>(40)</sup>.

Para Ernesto Villanueva <sup>(41)</sup> el hecho de no legislar específicamente en el sector de las SIC denota una negociación que privilegia un asunto político sobre una cuestión que debería ser estrictamente técnica; esto es porque, si bien es cierto que ya tenían una legislación previa, la Ley de Particulares es más positiva y tiene mayores elementos de garantía por lo que, en todo caso, se debió haber reformado la Ley de Sociedades de Información Crediticia para tenerla como una norma supletoria y no excluir a este sector del espíritu normativo de la nueva ley porque éste y los principios básicos de la legislación deben ser iguales para todos, puesto que no es posible distinguir y tener mayor protección en unos casos y menor protección en otros, por lo menos no se explica desde un punto de vista técnico.

---

<sup>(40)</sup> Cámara de Comercio, Servicios y Turismo de Monterrey, *El impacto de las nuevas tecnologías en las Empresas*, [En línea] <<https://comisionlegalcanaco.wordpress.com/2012/03/20/sociedades-de-informacion-crediticia-excentas-de-las-obligaciones-de-privacidad/>> [Consulta 24. feb. 2015].

<sup>(41)</sup> VILLANUEVA, Ernesto. Centro de Investigaciones Jurídicas Udlap. Puebla, México- Entrevista personal. Septiembre-2010.

Villanueva <sup>(42)</sup> explica que, en el caso de México, esta diferencia obedece a razones políticas porque cuando la ley se elaboró ya había sectores establecidos, como el sector bancario o el sector comercial, que generaron tensión: *“Cuando el comité de diseño está en la labor técnica ocurre que, al momento de la negociación en el Congreso, aparecen presiones de carácter político que provocan una legislación de aproximación sucesiva, lo cual es lamentable porque lo deseable es la existencia de una sola ley”*. En este caso se hablaría de integrar en una a la Ley de Sociedades de Información Crediticia, la LFPDPPP y la Ley Pública. Por el contrario, son tres leyes que regulan un mismo objeto y genera mayor burocracia, complicación y dificultad para el gobernado por tratar un mismo objeto y bien jurídico, que es precisamente la vida privada expresada mediante la protección de datos personales inherentes a las personas físicas y personas morales.

### **1.5.2. Instituto Nacional Electoral**

A partir de 1977 México inició una serie de reformas político-electorales que sirvieron como fundamento de la institucionalidad vigente. Entre estas reformas, una de las más solicitadas por los partidos de oposición al entonces partido hegemónico fue la conformación de un padrón electoral confiable, necesario para un procedimiento electoral democrático. Para Gómez y Ornelas <sup>(43)</sup> la creación de este instrumento originó cierta tensión entre el derecho a la protección a la privacidad en su vertiente de protección de datos personales y la protección de los derechos políticos de los ciudadanos.

El proceso de creación constó de varias etapas, involucró a ciudadanos, al Instituto Nacional Electoral y a los partidos políticos. Para Gómez y Ornelas <sup>(44)</sup> los ciudadanos tuvieron que entregar su información personal necesaria para conformar el padrón electoral, que contiene todos los ciudadanos mexicanos que solicitaron su inscripción a fin de obtener su credencial para votar con fotografía para ejercer su derecho al voto en 2009, que incluyó: nombre completo, lugar y fecha de nacimiento, edad, sexo, domicilio y tiempo de residencia, ocupación, firma, huella digital y su fotografía. A fin de que el padrón fuera lo más confiable posible y se eliminaran las inconsistencias, se involucraron los partidos políticos y los ciudadanos; esto supuso que los datos personales contenidos en las bases de datos se

---

<sup>(42)</sup> *Ídem.*

<sup>(43)</sup> GÓMEZ, A. y ORNELAS, L., *Protección de Datos Personales en México: el caso del Poder Ejecutivo Federal*. México: UNAM.

<sup>(44)</sup> *Ídem.*

divulgaran para que tanto los institutos políticos como los votantes pudieran corroborar su veracidad.

Los datos personales que el ciudadano proporciona actualmente al Instituto Nacional Electoral son tratados conforme a las obligaciones previstas en la Constitución Política de los Estados Unidos Mexicanos, en la Ley General de Instituciones y Procedimientos Electorales (LEGIPE) y en el artículo Cuarto Transitorio del Decreto de Reformas de la Ley General de Población, publicado en el Diario Oficial de la Federación el 22 de julio de 1992, referentes al tratamiento de los datos personales en los trámites de inscripción o actualización al Padrón Electoral, y en consecuencia la obtención de la Credencial para Votar e incorporación a la Lista Nominal de Electores, para ejercer su derecho al voto y contar con un medio de identificación personal.

Los ciudadanos podrán interponer escritos de queja cuando consideren que algún funcionario u órgano del Instituto, partido político, organismo electoral de entidades federativas, o cualquier sujeto con derecho a tener sus datos personales a través del Registro Federal de Electores, haga un tratamiento diverso a las finalidades establecidas en la Constitución y la LEGIPE.

El Instituto atenderá las solicitudes de cotejo, supresión y queja de los ciudadanos por el tratamiento de sus datos personales, conforme lo previsto en los Lineamientos para el Acceso, Rectificación, Cancelación, Oposición y Validación de Datos Personales en Posesión de la Dirección Ejecutiva del Registro Federal de Electores.

El Instituto recabará e incorporará en el Registro Federal de Electores los datos personales que forman parte del Padrón Electoral, que de conformidad con los artículos 140, numeral 1 y 156 del LEGIPE son proporcionados por los ciudadanos, siendo los siguientes:

1. Nombre(s)
2. Apellido paterno
3. Apellido materno
4. Sexo
5. Edad
6. Fecha y Lugar de Nacimiento
7. Domicilio
8. Entidad federativa, municipio y localidad que corresponde al domicilio
9. Tiempo de residencia en el domicilio
10. Ocupación
11. Firma

12. Fotografía
13. Huellas dactilares
14. Clave Única del Registro de Población
15. Número y fecha del certificado de naturalización, en su caso

Los documentos, datos e informes que los ciudadanos proporcionen al Registro Federal de Electores, en cumplimiento de las obligaciones que les impone la Constitución y el LEGIPE, no podrán comunicarse o darse a conocer, salvo cuando se trate de juicios, recursos o procedimientos en que el Instituto Nacional Electoral fuese parte, para cumplir con las obligaciones previstas por la Ley en materia electoral y por la Ley General de Población en lo referente al Registro Nacional Ciudadano o por mandato de juez competente<sup>(45)</sup>.

Los miembros de los Consejos General, Locales y Distritales, así como de las comisiones de vigilancia, tendrán acceso a la información que conforma el padrón electoral, exclusivamente para el cumplimiento de sus funciones y no podrán darle o destinarla a finalidad u objeto distinto al de la revisión del padrón electoral y las listas nominales.

### **1.5.3. Otras Bases de Datos.**

En una investigación periodística realizada por María de la Luz González de El Universal, en abril de 2010 <sup>(46)</sup> advirtió sobre la venta de bases de datos con información personal de millones de mexicanos por doce mil dólares en Tepito. De acuerdo con la reportera, que lo comprobó en tres memorias externas, el comprador puede adquirir el padrón electoral del país, el registro vehicular y de las licencias de conducir, los números de los teléfonos públicos del país, los datos de los policías también de todo el país (con la fotografía, número de placa y el lugar donde están adscritos), el parque vehicular del Servicio Federal, que incluye el transporte de carga, etcétera. Sumado a todo esto, destaca que esta información no sólo la utiliza el crimen organizado para extorsión, sino también agentes policíacos para “agilizar su trabajo” al rastrear llamadas relacionadas con secuestros o extorsiones realizadas desde teléfonos públicos, trámite que les tomaría aproximadamente cinco días si lo hacen conforme al procedimiento.

---

<sup>(45)</sup> INE, *Manifestación de Protección de Datos Personales recabados por Registro Federal de Electores* [En línea]: <http://www.ine.mx/archivos2/portal/credencial/datosPersonales.html>> [Consulta: 26. feb. 2015].

<sup>(46)</sup> González, Luz (2010). Tepito vende bases de datos oficiales. El Universal en línea. <http://www.eluniversal.com.mx/primer/34792.html>> [Consulta: 26. feb. 2015].

En entrevista, González <sup>(47)</sup> declaró que los vendedores de las bases de datos le aseguraron que estaban actualizadas a 2009, y ella pudo encontrar sus datos, los de familiares y personas cercanas en el padrón que vendían para corroborar la información.

Sobre la manera ilícita en la que obtienen las bases de datos, agregó que: “Ellos compran las bases de datos a la gente que trabaja en las dependencias, a cualquier empleado que tenga acceso a las bases de datos, no tiene que ser el titular del área, con que sepa sustraer la información es suficiente porque no hay candados, desafortunadamente en nuestro país no tenemos esta cultura de protección de datos” añadió que el caso del padrón resulta muy preocupante “no se sabe de dónde se filtró esa base de datos, el INE dice que no fue de ahí y jura que el registro tiene candados, pero no conocemos cuáles son esos candados. Realmente se ignora cómo resguardan la información que das para un simple trámite porque todas las bases de datos que puedas imaginar están al acceso del crimen organizado: tienen registros de bancos, de escuelas, etcétera.

Otro caso que le parece preocupante son los partidos políticos porque cuando piden una copia del padrón se les da, “...y de ahí no sabes cuántos más la tienen, qué seguridad tiene el director del partido político, el director de elecciones, etcétera, sobre esas bases de datos que han sido tan cuidadosamente elaboradas, que han costado tanto trabajo integrar, qué pasa cuando se entregan las copias. Estas averiguaciones dejan al descubierto la problemática que hay en México en cuanto a la falta de confiabilidad en las bases de datos almacenadas por el gobierno, que son tan vulnerables de robo y fugas de información. Es necesario cuestionar a las autoridades responsables de esa información para saber por qué se quebranta con tanta facilidad su seguridad y cómo es que no resultan responsables.

#### **1.5.4. Sector Salud.**

El presente apartado se enfocará a resaltar la importancia que tiene la debida protección de los datos personales relativos a la salud, para Lina Ornelas <sup>(48)</sup> *es toda aquella información sobre estados físicos y mentales concernientes a una persona física identificada o identificable*. En México, los prestadores de los servicios de salud están clasificados en

---

<sup>(47)</sup> *Ídem.*

<sup>(48)</sup> ORNELAS Núñez, Lina, *Segundo Seminario Internacional: Acceso a la Información y protección de datos personales* [En línea]:[http://www.infodf.org.mx/iaipdf/informes/informe2008/anexos/Capitulo\\_5/Seminario/Lina\\_Ornelas.pdf](http://www.infodf.org.mx/iaipdf/informes/informe2008/anexos/Capitulo_5/Seminario/Lina_Ornelas.pdf)> [Consulta: 28. feb. 2015].

tres rubros: seguridad social, servicios médicos privados y servicios de población abierta. Por ello, resulta imprescindible contar con una regulación comprehensiva para evitar un mal manejo de la información, que conlleve injerencias arbitrarias o ilegales a la vida privada de las personas, así como la utilización de los datos personales para fines distintos por los que fueron recabados en primera instancia. El dato de salud, por su naturaleza, es considerado como un dato sensible y como al resto de los datos personales les son aplicables los principios de protección internacionalmente reconocidos, además de que se debe contar con medidas de seguridad más altas que garanticen la confidencialidad, integridad y disponibilidad de dicha información.

Se carece de una regulación comprehensiva que regule específicamente el tratamiento o manejo de datos de salud, que evite un mal manejo de dicha información. <sup>(49)</sup>

- La falta de observancia de los principios de protección de datos reconocidos internacionalmente en las instituciones de salud públicas y privadas.
- La ausencia de homogeneidad en la organización, manejo y conservación de archivos clínicos.
- La posesión de datos de salud debe obedecer exclusivamente a las atribuciones legales de los entes públicos, o a la legitimación derivada del servicio entre hospitales privados y pacientes.
- Los datos de salud deben tratarse únicamente para la finalidad para la cual fueron obtenidos.
- Los datos de salud deben ser exactos, adecuados pertinentes y no excesivos.
- Los datos deben almacenarse de forma tal que permitan el ejercicio de los derechos de acceso y rectificación.
- Se debe hacer del conocimiento del titular de los datos de forma escrita, al momento de recabarlos, el fundamento y motivo de ello, así como los propósitos para los cuales se tratarán los mismos.
- Los datos de salud deben contar con medidas de seguridad necesarias para garantizar su integridad, confiabilidad, confidencialidad y disponibilidad de la información.

---

<sup>(49)</sup> *Ídem.*

- Toda transmisión de datos de salud, debe contar con el consentimiento previo, por escrito y otorgado de manera libre por parte del titular, salvo las excepciones legales conducentes.

En este orden de ideas, de acuerdo con la Norma Oficial Mexicana NOM-168-SSA1-1998, se entiende por expediente clínico al “conjunto de documentos escritos, gráficos e imagenológicos o de cualquier otra índole, en los cuales el personal de salud, deberá hacer los registros, anotaciones y certificaciones correspondientes a su intervención, con arreglo a las disposiciones sanitarias”; también define un resumen clínico como un “documento elaborado por un médico, en el cual se registrarán los aspectos relevantes de la atención médica de un paciente contenidos en el expediente clínico. Deberá tener como mínimo: padecimiento actual, diagnósticos, tratamientos, evolución, pronóstico, estudios de laboratorio y gabinete”. La norma establece que los prestadores de servicios médicos del sector público, social y privado deben elaborar y conservar el expediente clínico por un periodo mínimo de 5 años, mismo que debe contener los siguientes datos generales del usuario: nombre, sexo, edad y domicilio. Toda la información contenida pertenece a la institución prestadora del servicio médico y podrán otorgarla únicamente con una solicitud por escrito por el paciente, familiar, tutor, representante y autoridades sanitarias, ya que se trata de información confidencial (NOM-168-SSA1-1998).

A pesar de que la norma menciona que la información contenida en el expediente clínico debe ser manejada con discreción y confidencialidad, se atiende únicamente al cumplimiento de los principios científicos y éticos que orientan la práctica médica, mas no implica una sanción a quien haga un uso diferente o inapropiado de ella.

Por otro lado se encuentran los lineamientos establecidos por la Ley General de Salud en Materia de Prestación de Servicios de Atención Médica referentes al derecho a la información perteneciente a los usuarios de los servicios de salud, entre estos derechos se encuentran los siguientes:

El artículo 29 habla sobre la obligación que tiene todo profesional de salud de proporcionar al usuario, familiares, tutor o representante legal, la información completa sobre el diagnóstico, pronóstico y el tratamiento que corresponda; al igual que la NOM-168, en su artículo 32 establece que deben conservar los expedientes clínicos de los usuarios por un

periodo mínimo de cinco años. En este mismo sentido, la Ley General de Salud, artículo 77 bis 37 establece ciertos derechos con respecto a la confidencialidad y a la información:

- Recibir información suficiente, clara, oportuna y veraz, así como la orientación que sea necesaria respecto de la atención de su salud y sobre los riesgos y alternativa de los procedimientos diagnósticos, terapéuticos y quirúrgicos;
- Contar con su expediente clínico;
- Ser tratado con confidencialidad;

El principal problema de la NOM-168 recae en que muchos médicos del sector público y privado no lo llevan como debe ser, se ha creado la controversia de quién es el dueño del expediente clínico si el paciente, el médico o la institución. El expediente clínico es una información que puede usarse para afianzar diagnósticos, en casos académicos para la enseñanza o para la investigación. Un expediente clínico bien llevado puede servir mucho. También es importante porque constituye la única defensa que el médico tiene ante cualquier demanda, ya que lo primero que pide el ministerio público es el expediente y no se le puede agregar ni quitar nada. Además de la historia clínica con antecedentes, notas de evolución, de laboratorio, el gabinete, etcétera, también debe llevar el consentimiento informado que es lo más importante.

El sector salud en nuestro país ha dado pasos para garantizar la seguridad de los datos personales, incluso Argentina señaló el avance que hay en México, sin embargo, el trato inicial de éstos recae en los médicos que realizan el expediente clínico y en su ética profesional para cumplir con lo establecido por las normas, leyes y reglamento.

#### **1.5.5. Sector Educativo.**

Otro sector en donde era urgente la protección de los datos personales era el educativo. De acuerdo con Ciscomani <sup>(50)</sup>, en México hay más de 26 mil escuelas privadas y más de 190 mil escuelas oficiales. El uso erróneo de datos personales en posesión de las instituciones educativas puede provocar marginación, discriminación y restricción del acceso de los estudiantes a mejores oportunidades formativas. Por esta razón, Francisco Ciscomani, durante su exposición dentro del marco del VIII Encuentro Iberoamericano de

---

<sup>(49)</sup> CISCOMANI, Francisco, (2010). *Apertura del VIII Encuentro Iberoamericano de Protección de datos personales*. 29 de septiembre de 2010. Organizado por el IFAI, México. Versión estenográfica disponible en <http://viiiencuentroiberoamericano.ifai.org.mx/index.php/material>. [Consulta 28. feb. 2015].

Protección de Datos Personales, manifestó que la regulación y cooperación con el órgano garante era urgente.

El Registro Nacional de Alumnos concentra información de alrededor 25 millones de estudiantes, además del registro oficial de documentos académicos y de certificación, que constituyen un buró de documentos académicos con más de 30 millones de datos, constancias, certificados y títulos emitidos en los diferentes niveles educativos, mismos que, según Ciscomani fueron inscritos en 2009 en el Sistema Persona del IFAI.

Estas bases de datos, conformada por información de alumnos, familias y empleados, demandan una total protección puesto que abarca una tercera parte de la población nacional y se trata de un sector muy vulnerable que incluye menores de edad.

Entre las medidas que la Secretaría de Educación Pública toma para proteger los datos personales en posesión de las instituciones educativas está la elaboración de normas de control escolar, con criterios mínimos que deberán ser adoptados en los centros educativos por las autoridades escolares, así como una próxima creación de un Manual de Uso y Protección de Datos en centros escolares.

Es muy importante que, además de las leyes establecidas, las instituciones educativas se inclinen por proteger la información de sus alumnos y asimismo funjan como instructores en la materia para crear una cultura de autoprotección.

#### **1.5.6. Sector de Telecomunicaciones.**

Hablar de las telecomunicaciones es hablar de las tecnologías de la información que han revolucionado el tratamiento de los datos personales. El Instituto Federal de Telecomunicaciones fue creado para coordinar el espectro radioeléctrico nacional, a través de las telecomunicaciones, radiodifusión y operación de cadenas de televisión restringida; así como las redes telefónicas. Teniendo a su cargo la regulación, promoción y supervisión del uso, aprovechamiento y explotación del espectro radioeléctrico, las redes y la prestación de los servicios de radiodifusión y telecomunicaciones, así como del acceso a infraestructura activa, pasiva y otros insumos esenciales.

En este marco, los principales exponentes de esta idea Jose Luis Piñar Mañas y Lina Ornelas Núñez <sup>(51)</sup>, consideran las herramientas que aportan las telecomunicaciones y el Internet, insustituibles a la hora de mejorar la productividad, la conectividad y la competitividad de la sociedad del Siglo XXI, cuentan desde ahora con principios esenciales para desarrollarse con certeza jurídica, con reglas constitucionales explícitas, con reglas más claras para dar tratamiento a datos personales y con un órgano regulador con experiencia que es el IFAI. La subsecuente reglamentación del novel marco mexicano tendrá que reconocer que México requiere de un marco estratégico para el desarrollo de la Sociedad de la Información que, en el ámbito telecomunicaciones, debe garantizar diversas cuestiones, como lo es la armonización del respeto a la intimidad y la privacidad en el ambiente digital, con el derecho al acceso universal a Internet. Y éste otro derecho requiere de un marco legislativo y de políticas públicas que no inhiba el fomento de las tecnologías y el desarrollo de nuevos servicios y redes.

Un amplio número de Empresas nacionales y extranjeras que inciden en México vienen poniendo en práctica políticas de privacidad en el terreno de los servicios de telefonía, Internet y una extensa gama de servicios de comunicación electrónica, pues no es un asunto que sea nuevo ya que se trata de tutelar derechos consagrados desde hace tiempo en la Declaración Universal de los Derechos Humanos adoptada por la Organización de las Naciones Unidas (en adelante ONU) y por varios otros instrumentos internacionales sobre derechos civiles y políticos. Pero al darse la categoría constitucional en nuestro país y contar con dos ordenamientos especializados: la LFPDPPP de 2010 así como el Reglamento de 2011 de ésta última, los individuos podrán ejercer sus derechos para proteger su vida privada e intimidad. <sup>(52)</sup>

Aunque de este modo México muestra una evolución en esa materia, otras naciones continúan haciendo esfuerzos por aprobar Directivas especializadas y exigir que derechos humanos y desarrollo de las TIC vayan de la mano.

---

<sup>(51)</sup> PIÑAR, José Luis y ORNELAS, Lina, *La Protección de Datos Personales en México*, México, D.F., Ed., Tirant Lo Blanch México, 2013, p. 422.

<sup>(52)</sup> *Ídem*

### 1.5.7. Internet.

Por otro lado aparece un nuevo reto en el sector: Internet. Éste se ha convertido en una herramienta muy útil a la que se han trasladado actividades comerciales, sociales, trámites de gobierno, etcétera. Esta dinámica reciente ha originado gran preocupación por el riesgo que implica para la privacidad, puesto que, como explicó De la Parra <sup>(53)</sup> durante su participación en el VIII Encuentro Iberoamericano de Protección de Datos, la información proporcionada es muy detallada, individualizada y sujeta a procesamiento de forma masiva. También cuenta con información como el IP, que da información sobre el navegador, potencialidades, aplicaciones ejecutadas, tiempo y fecha de visita.

El comercio electrónico representa una de las inquietudes para la seguridad de la privacidad. Sin embargo, es una gran herramienta porque elimina las barreras geográficas y reduce la necesidad de intermediarios. Por esta razón, la protección en la red cobra vital importancia para incentivar la actividad económica dentro del mercado digital.

Calderón M., expuso <sup>(54)</sup> que según datos del Banco Mundial: “un incremento en la penetración de diez por ciento del mercado de banda ancha representa un incremento del uno por ciento del Producto Interno Bruto (en adelante PIB), y México, desgraciadamente, hoy tiene una de las penetraciones más bajas de Internet del mundo, más reducida que todos los países de la Organización para la Cooperación y el Desarrollo Económicos (en adelante OCDE) y de las más bajas si lo comparamos contra los homólogos de otros países latinoamericanos.

El comercio electrónico representa una de las inquietudes para la seguridad de la privacidad. Sin embargo, es una gran herramienta porque elimina las barreras geográficas y reduce la necesidad de intermediarios. Por esta razón, la protección en la red cobra vital importancia para incentivar la actividad económica dentro del mercado digital.

---

<sup>(53)</sup> PARRA, R. *La protección de datos en el sector de las telecomunicaciones*. Panel presentado en el VIII Encuentro Iberoamericano de Protección de Datos Personales en septiembre de 2010, organizado por el IFAI, México. Versión estenográfica disponible en <http://viiiencuentroiberoamericano.ifai.org.mx/index.php/material>. [Consulta 2. mar. 2015].

<sup>(54)</sup> CALDERÓN, M. (2010). *La protección de datos en el sector de las telecomunicaciones*. Panel presentado en el VIII Encuentro Iberoamericano de Protección de Datos Personales en septiembre de 2010, organizado por el IFAI, México. Versión estenográfica disponible en <http://viiiencuentroiberoamericano.ifai.org.mx/index.php/material> [Consulta 2. mar. 2015].

Así es que la protección de los datos en la red es un elemento clave para promover este sector porque, a opinión de Calderón <sup>(55)</sup>, si los usuarios se sienten seguros de hacer transacciones utilizarían más Internet. Sin embargo, también considera que una sobrerregulación tampoco es conveniente porque ocasiona la pérdida de competitividad en el mercado desarrollado mediante las tecnologías de la información. Por esta razón, Calderón se pronuncia a favor de “una regulación adecuada necesaria para consolidar la confianza de los usuarios en este ambiente digital e incrementar su uso y cantidad de servicios... con soluciones compatibles a regulaciones internacionales”. Esto último es importante porque Internet es una red global y podría ser problemático que la normativa mexicana difiriera mucho de la normativa de otros países.

El consentimiento del usuario debe ser indispensable, y para Calderón esto es una dicotomía porque muchas veces el usuario se preocupa por el uso de sus datos personales a la vez que, con gran facilidad, proporciona demasiada información sobre sí a las redes sociales.

Cada sitio web cuenta con políticas de privacidad en los que establecen cláusulas sobre el uso que harán de los datos personales, el fin para el que los recopilan y su transmisión a terceros, que los usuarios generalmente aceptan sin leer para poder registrarse y realizar alguna operación.

#### **1.5.8. Redes Sociales: Facebook.**

Las redes sociales son una **fuentes de acceso público**, por ello la misma ley permite el uso de los datos que ahí se viertan mientras haya consentimiento de quienes se registran; sin embargo, esto expone a los usuarios a la venta o utilización comercial de la información, extorsiones y robo de identidad.

La cantidad de mexicanos expuestos alcanza 50 millones que, por lo menos, son usuarios de una red social como Facebook, según datos de la misma Asociación Mexicana de Internet. Hasta nueve de cada 10 internautas accede a una red social; del resto que no cuenta con un perfil, tres de cada 10 se abstienen por protección a sus datos personales.

La presidenta del Instituto Federal de Acceso a la Información (IFAI), Ximena Puente de la Mora, ha lamentado que las reglas de privacidad no dependan del Estado mexicano

---

<sup>(55)</sup> *Ídem*

sino de las mismas Empresas. Ha explicado que cuando se aceptan las condiciones, el usuario se somete a esas reglas y la información es pública.

Por su parte, el investigador y consultor en Opinión Pública y Ciencia Política de la Universidad del Valle de Atemajac, Alberto Gómez Ramírez, señala que es preocupante el dominio de las compañías sobre los datos en las plataformas. El beneficio que tienen las Empresas es la utilización de toda la información de los usuarios. Describe que las bases de datos con toda la información de los usuarios se vende a las compañías comercializadoras para planificar campañas de acuerdo a los perfiles de los usuarios: “Es así como se utiliza con fines comerciales la información que proporcionas, el principal interés de las Empresas”.

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares establece que no se requiere consentimiento de las personas para el tratamiento de datos personales cuando los datos “figuran en fuentes de acceso público”, como se establece en las condiciones del servicio de las redes sociales.

En mayo de este año comenzó a funcionar, por petición del Tribunal de Justicia de la Unión Europea, el derecho al olvido que implica la desaparición de datos personales en Internet.

La legislación se origina por un español que aparecía mencionado como moroso en una página de Internet en el año 1998. Poco después saldó sus deudas pero eso ya no aparecía en la web. Por este hecho, el Tribunal europeo ordenó la creación de una herramienta que permita a las personas la remoción de sus datos en las páginas web dentro de los resultados de un buscador. Los links continúan ahí pero Google los desaparece.

Las personas que soliciten este derecho deben fundamentar las razones de su petición para cada link que quieran que desaparezca. Google analiza la petición una por una, y decide a quién sí otorgarle el olvido. La herramienta puede observarse en esta liga: <http://is.gd/JL84Ht>.

Hasta ahora la medida sólo es activa en el continente europeo y en algunos países de Sudamérica. En México, el Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), mostró su apertura para adoptar esta medida. Y con el fin de acelerar las gestiones, en noviembre del año pasado, informó que envió al Congreso dos propuestas para fortalecer el marco normativo en materia de protección a datos personales.

## CAPÍTULO SEGUNDO

### DATOS PERSONALES Y COMUNICACIÓN PÚBLICA EN MÉXICO

Pareciera que la protección de datos personales corresponde únicamente al ámbito del Derecho. Sin embargo, es necesario destacar que el campo político está intrínsecamente relacionado con la Comunicación puesto que le otorga un espacio para su aparición. Por lo tanto, este derecho nuevo en nuestro país debe hacer uso de las herramientas que la Comunicación Pública ofrece para desarrollarse y coexistir junto con otros derechos. Este capítulo está dedicado a estudiar la relación que existe entre la Comunicación Pública y el Derecho a la Protección de los Datos Personales y su aplicación práctica en los sectores contenidos por la Ley para la creación de políticas públicas.

Según la teoría de sistemas de Niklas Luhmann la sociedad se comprende a partir de la comunicación, la cual representa el elemento clave para que pueda existir tal sociedad. Las acciones y las estructuras son posibles en tanto son posibles de ser comunicadas. <sup>(56)</sup> Ésta comunicación se compone del acto de comunicar, de la información y de la comprensión. Este proceso supone códigos que varían dependiendo del -sistema social- al que se refiera, ya sea la educación, la política o la economía. Son estos sistemas sociales, entidades analíticas, las que permiten observar el acontecer en la sociedad. Ninguno de estos tres elementos es contenido en sí mismo, sólo son selección de posibilidades en un circuito: el acto de comunicar es motivo e intenciones, la información es horizonte de posibilidades derivadas de las intenciones del acto, mientras que la comprensión es aceptación o rechazo de la comunicación.



<sup>(F4)</sup> Fuente: Acoplamiento estructural entre tres sistemas. Glosario sobre la teoría social de Niklas Luhmann (pp. 19–21). México: Universidad Iberoamericana-ITESO/Anthropos

<sup>(56)</sup> NIKLAS, Luhmann. Traducción Gaytán Alcalá Felipe. *Notas Críticas. Teoría de sistemas, la autoobservación de la sociedad moderna*. Editorial Alianza. 2002. p. 657.

(F4) Diseño Diana Márquez Cisneros

A diferencia de la sociología, la teoría de sistemas plantea una nueva forma de observar lo social aceptándolo como un estudio complejo abierto a variantes en todas las posibilidades de actuar de la sociedad y no como un proyecto cuadrado regido por normas. **Contingencias** es la palabra clave para entender el enfoque de la teoría de sistemas, el cómo se construye la sociedad.

La teoría tiene como base el análisis de la relación entre los sistemas y los entornos y lo que sucede dentro de los sistemas. Para su observación, la cual se determina de segundo grado, es decir, que hace una doble observación: al observar cómo observan los sistemas e implicar su punto ciego; utiliza el método de las equivalencias funcionales la cual consiste en observar todas las posibilidades o contingencias y estudiar la selección final del sistema.

Para Luhman la sociedad es comunicación; la cual es observable en la doble contingencia de alter y ego. Una persona por sí misma no comunica sino que solo tiene ideas; comunica cuando alguien más comprende su idea ya sea que este último sujeto la acepte o la rechace, lo cual enriquece la contingencia. <sup>(57)</sup>

Como ya lo mencioné, cada sistema tiene su código o bien doble contingencia; por lo que se puede decir que actúan solo en su código y así es como se distinguen de los otros sistemas. Los sistemas son per se comunicación y a su vez estos constituyen a la sociedad. Cada sistema recibe del entorno comunicaciones que acepta o rechaza. Entre sistemas también pueden verse en situaciones en las que se conecten momentáneamente de forma que “co-evolucionan”. En el interior de cada sistema hay tres dimensiones que les permiten actuar: Dimensión temporal, objetiva y social; bajo estas dimensiones, los sistemas procesan información del entorno y generan más diferencias en su interior.

De esta manera, la teoría de sistemas se convierte en un observador de la sociedad moderna posibilitando la observación de observaciones al observar cómo observan los diferentes sistemas sociales. Con esta observación de segundo orden se puede comprender la contingencia y complejidad de lo social. A final de cuentas, como dice el autor, lo que entendemos como realidad es sólo la observación de observaciones. La teoría de sistemas posibilita la autoobservación de la sociedad moderna sobre sus posibilidades y selecciones.

---

<sup>(57)</sup> *Íbidem*, p. 664.

## 2.1. Comunicación Pública, Espacio Público y Democracia.

Para comprender más la comunicación pública es conveniente estudiar los dos conceptos por separado. Existen diferentes definiciones y teorías referentes a la Comunicación, Ferrer <sup>(58)</sup>, expresa que la comunicación es todo el testimonio de las relaciones humanas. Expone distintas explicaciones para la comunicación. Por mencionar algunas, Schramm la entiende como el acto que forma parte de la función viviente de la sociedad; para Aranguren es la transmisión de información con vistas a una respuesta; Ruesch afirma que es un modelo científico que permite explicar aspectos físicos, intrapersonales, interpersonales y culturales de los sucesos; Berlo la entiende como un proceso dinámico que avanza sin tener punto de partida ni final; Shanon y Weaver la vislumbran como un proceso mediante el cual una mente influye en otra; Moles afirma que es un acercamiento global que puede explicar la totalidad de nuestro mundo; MacBride escribe que es una facultad acumulativa y que cada lenguaje nuevo se suma al anterior sin eliminarlo.

Todas las definiciones anteriores vislumbran a la comunicación como un proceso dinámico necesario para el desarrollo de la humanidad. Ferrer agrega el factor del entendimiento, de tal manera que la define como: “el proceso que lo vuelve respuesta, cerrando el círculo significativo del que habla al que escucha. Si las palabras son el reflejo de las cosas, la comunicación es el reflejo de su entendimiento”. Por esto, “la comunicación nace de la necesidad y el deseo de hacer común lo que debe entenderse”, ya que una idea o un conocimiento es útil cuando puede comunicarse con el fin de estar al servicio del entendimiento común para acortar la diferencia entre todo y entre todos. De forma más explícita, Ferrer <sup>(59)</sup> señala con referencia a la comunicación que:

*A partir de su origen, la comunicación es diálogo directo del hombre con el hombre en todo su repertorio de intercambios, incluidos los más elementales. La comunicación es el medio de los medios, en la medida en que a ella afluyen todos los conocimientos y los descubrimientos del hombre para hacerse comprensible entre sí y hacer comprensible cuanto le rodea. La comunicación está en el centro de todo lo perceptible, pero sobre todo como conciencia humana de la vida en común y de su cultivo. En tanto que vía de reciprocidad, fundamenta el equilibrio social. No hay cooperación, ni participación sin comunicación. A falta de ésta, la*

---

<sup>(58)</sup> FERRER, E., **Comunicación y Comunicología**, México, D.F., Ed., Eufesa, México, 1982, p. 14.

<sup>(59)</sup> *Ídem.*

*comunidad no funciona o se encuentra enferma... Hay que entender que la comunicación es un ejercicio garantizado por la libertad.*

Con esto, el autor sitúa a la comunicación como el medio que da espacio y cabida al desarrollo de distintos conocimientos para alcanzar la conciencia humana en la búsqueda de un bien común, y obtener un equilibrio social de cooperación y participación con base en el ejercicio de la libertad que posee cada individuo. Para Ferrer, un pueblo sin comunicación es un mero esqueleto ya que ésta no es sólo su reflejo sino parte de su esencia que lo hace más sólido debido a que amplía la participación común, enseña a adaptarse al cambio y, en ocasiones, también lo promueve.

Desde esta perspectiva, Ferrer escribe que la comunicación tiene un origen y carácter social que va más allá de un mero intercambio de signos. Es un proceso activo y continuo con manifestaciones humanas de distintos niveles. El propósito principal de la comunicación está inmerso en la raíz de su propio término: ser en común, poner en común. Por lo tanto, se refiere a la interdependencia del uno con el otro y de los demás con todos y, en este sentido, lo común, la comunicación y la comunidad convergen.

Por otra parte está el término “público”. Uno de los usos con mayor predominio de éste es el que da su raíz latina publicus, derivada de poplicus o populus, que quiere decir “el pueblo” según Price <sup>(60)</sup>. Monzón <sup>(61)</sup> explica que la esfera de lo público se refiere a las actividades públicas en las que el ciudadano puede participar libremente como actividades cívicas y comunes, en donde ocurre la publicidad como el espacio en donde la libertad, diálogo y claridad son posibles.

Al juntar ambos términos en lo que es la comunicación pública, podemos encontrar que se trata de un proceso regido por la libertad que da cabida al pueblo para que participe en actividades que busquen el desarrollo del bien común dentro de un espacio abierto. Según Beauchamp la comunicación pública es:

*El conjunto de fenómenos de producción, tratamiento, difusión y retroacción de la información que refleja, crea y orienta los debates y los temas públicos; la comunicación pública entendida no solamente como el quehacer de los medios, sino también de las instituciones, las*

---

<sup>(60)</sup> PRICE, Vicent, *Opinión Pública*, México, D.F., Ed., Paidós, México, 1994.

<sup>(61)</sup> MONZÓN, Cándido, *Opinión pública, comunicación y política*, Madrid, Ed., Tecnos, 1996.

*Empresas, los movimientos y los grupos que intervienen en la plaza pública (Demers y Lavigne).* <sup>(62)</sup>

Esta definición vislumbra el espacio común en el que se realiza la comunicación al que llamaron “plaza pública”, escenario en donde ocurren los debates sobre temas que interesan o afectan a la comunidad. La comunicación pública no pertenece únicamente a los medios de comunicación mediante los cuales se dan a conocer los acontecimientos, sino que, en su definición, relaciona el espacio de la plaza pública con la actividad de todas las instituciones, ya sean privadas o gubernamentales, que afectan el quehacer de la colectividad. Esta plaza es un espacio abierto a todo el mundo en donde predomina la libertad y la igualdad en donde se orientan los temas de interés general. Monzón menciona tres modelos de espacio público existentes: griego, ilustrado y sociedad de masas. El modelo griego remite al ágora en donde los ciudadanos se reunían para hablar asuntos relacionados con el gobierno de la ciudad en donde coincidían la política y la esfera pública. El modelo ilustrado explica el salto desde la esfera privada a la pública que los separa, en donde en la esfera privada dominaba la conciencia individual y la opinión y la esfera pública pertenecía a la razón de Estado. En este modelo la razón de Estado está sujeta a la razón del público que pide explicaciones de la administración del bien común, es decir, se habla de los primeros orígenes de la opinión pública. Por último, el tercer modelo está marcado por la aparición de las sociedades de masa y los medios de comunicación en el que la opinión pública que antes era de sabios e ilustrados, se convierte en una opinión imperfecta basada en juicios manipulados u opiniones segmentadas.

Demers y Lavigne <sup>(63)</sup> explican que la comunicación pública permite el desarrollo de teorías y métodos útiles para distintas disciplinas, así como técnicas procesos y métodos adecuados para los profesionales que producen los mensajes públicos y la intervención comunicacional. Cuando el espacio público se centra en el debate privilegia la discusión racional de temas públicos y anuncia su degradación debido a la industrialización y comercialización de los medios de comunicación, periodismo e información, aunque también puede apuntar hacia el debate en un sentido metafórico sin mermar la seriedad de los temas ni de los medios. Una característica más que señalan sobre la comunicación pública y el

---

<sup>(62)</sup> DEMERS F. y LAVIGNE, A., *La comunicación pública: una prioridad contemporánea de investigación*. Novena Época, núm. 7, enero-junio, 2007, p.65.

<sup>(63)</sup> *Ídem*.

espacio público se centra en que el espacio público designa objetos reagrupados en un territorio físico como principio de clasificación y la comunicación pública gestiona temas colectivos sostenidos por la circulación de información y opiniones, es decir, no se vislumbra como la plaza pública sino por contribuir con la opinión pública para la toma de decisiones y realización de acciones gubernamentales y estatales.

Según explican Demers y Lavigne, en la década de los ochenta surgieron las “sociedades de relaciones públicas generalizadas”, que eran grupos de interés diversos y organizados que participaban en la actividad democrática para enriquecerla. De estos grupos organizados nació la “sociedad civil”, que agrupaba actores sociales no estatales del sector no mercantil y representaba a distintos asuntos públicos con presencia en debates con cierto grado de responsabilidad social. En resumen, la comunicación pública surgió como parte del debate público en las democracias modernas y se alía con el derecho en la defensa del bien común en su carácter de socialmente responsable.

Estos casos presentados, de acuerdo con Muhlmann, citado por Demers y Lavigne, convergen y dan apertura en los regímenes políticos democráticos sobre las libertades de opinión, expresión y prensa que median la crítica pública de las acciones del Estado y sobre las deliberaciones públicas referentes a la administración colectiva. Esto quiere decir que la comunicación pública, el espacio público y el espacio público mantienen un mismo concepto en común, lo “público” conserva su mismo sentido e intención de reivindicar la transparencia y eliminar el secreto de Estado para la construcción de las democracias modernas. Así como existen los derechos de tercera generación, también existe una democracia de tercer tipo en la que se involucra a los medios de comunicación junto con otros componentes sociales como grupos de presión, asociaciones, grupos minoritarios que compiten entre sí, crean alianzas, colaboran o se contraponen, con apoyo o sin apoyo del Estado para participar o no en las decisiones de éste. Desde esta perspectiva, se habla de una sociedad civil organizada para desempeñar un papel entre las fuerzas sociales (Demers y Lavigne).<sup>(64)</sup>

Estas agrupaciones sociales no recurren al uso de la fuerza sino a la comunicación pública, será interesante analizar cómo la protección de datos personales surgió a partir de la organización de un grupo minoritario de la sociedad civil que decidió hacer uso práctico

---

<sup>(64)</sup> *Ídem.*

del espacio público para hacer surgir un derecho reconocido ante el Estado, así como las distintas políticas públicas creadas a partir de entonces.

Otra característica de esta democracia de tercera generación es el uso que hace de las nuevas tecnologías de la información y los medios como espacio público para dar a conocer sus temas en cuestión y ponerlos al alcance de una comunidad aparentemente ilimitada que puede retroalimentar con su participación en los debates abiertos. Asimismo, como es propio de una democracia que hace posible la igualdad mediante el voto universal, la de tercera generación otorga al individuo su derecho de ser visible públicamente para dar tratamiento a su opinión o creencias así como se otorga esta oportunidad al especialista, representante popular o al experto. En otras palabras, el individuo se empodera de su identidad pública que contribuye con la formación de la democracia (Demers y Lavigne).

En ese orden de ideas, los medios acaparan grandes masas de la población. Esto origina que las personas sobre las que los medios inciden tienen la capacidad, a su vez, de influir en otras como una reacción en cadena. Este hecho trasciende porque de esta manera los medios pueden contribuir a crear crítica, rebeldía e inconformidad encausadas para analizar el poder y exigir cuentas.

Los medios realmente comprometidos pueden contribuir con la construcción de la democracia en su actividad diaria, siempre y cuando no caigan en la dinámica como la que tienen las dos grandes Empresas mexicanas, Televisa o TV Azteca. Existe una relación intrínseca entre la Comunicación y la Democracia porque el derecho de la información que consagra el artículo 19 de los Derechos Humanos se refiere, precisamente, al derecho que las personas tienen a informar, ser informados y a tener acceso a la información pública, puntos que tienen mucho que ver con la construcción de la democracia. Con el Decreto de Reforma Constitucional en Telecomunicaciones se ha determinado que la radiodifusión es un servicio público de interés general y que corresponde al Instituto Federal de Telecomunicaciones (en adelante IFT) el otorgamiento de Concesiones del espectro radioeléctrico en dicha materia y que éstas, cuando su uso es comercial, serán otorgadas mediante licitación pública. <sup>(65)</sup>

---

<sup>(65)</sup> Instituto Federal de Telecomunicaciones, *IFT-1 Licitación de dos cadenas de televisión radiodifundida digital* [En línea]: <http://portalanterior.ift.org.mx/iftweb/industria-intermedia/unidad-de-sistemas-de-radio-y-television/licitaciones-en-curso-radio-y-television/licitacion-ift-1/> [Consulta: 26. mar. 2015].

En ese tenor, la Constitución ha mandado al IFT publicar las Bases y Convocatorias para licitar nuevas concesiones de frecuencias de televisión radiodifundida que deberán ser agrupadas a efecto de formar por lo menos dos nuevas cadenas de televisión con cobertura nacional.

El presidente de México, Enrique Peña Nieto, calificó a la reforma como un “poderoso instrumento” para traer prosperidad al país y garantizó que los cambios en el sector salvaguardan la libertad de expresión en los distintos medios de comunicación, incluido Internet. Al promulgar la Ley Federal de Telecomunicaciones y Radiodifusión, se anuncia la creación de una nueva cadena de televisión pública bajo el nombre de “Sistema de Radiodifusión del Estado Mexicano” que se suman a la apertura en el sector a través de la licitación de dos nuevas cadenas de señal abierta. Con estas adecuaciones se asegura que “las dos nuevas cadenas -que serán licitadas- compitan en igualdad de condiciones” con las existentes.<sup>(66)</sup>

Todo esto permite la participación ciudadana que, en esta medida, podrá ser una sociedad más activa y el gobierno tiene el deber de incluir a los ciudadanos y tomarlos en cuenta para fomentar democracias sólidas.

## **2.2. Los Medios de Comunicación como Espacio Público.**

Demers y Lavigne<sup>(67)</sup> mencionan una idea sobre la cual es necesario reflexionar. El concepto de comunicación pública surgió de la necesidad de construir una relación entre la democracia y los medios de comunicación en los años ochenta, que hasta ese momento eran los medios tradicionales como la radio y las cadenas de televisión, ya que las nuevas tecnologías dieron un giro a la comunicación que abrió sus fronteras para dar un salto a la globalización y a los medios transnacionales. Este punto es importante desde dos perspectivas. Primero, como se analizó anteriormente, los medios son un espacio que pueden dar cabida a lo público para fortalecer las democracias, a la vez que, como sistema mercantil, poseen información que puede ser traducida en mercancía que, en ocasiones, no debe ser difundida sino conservar su confidencialidad. Esta ambivalencia de los medios va en función de que, por un lado, son difusores de información para el establecimiento de la

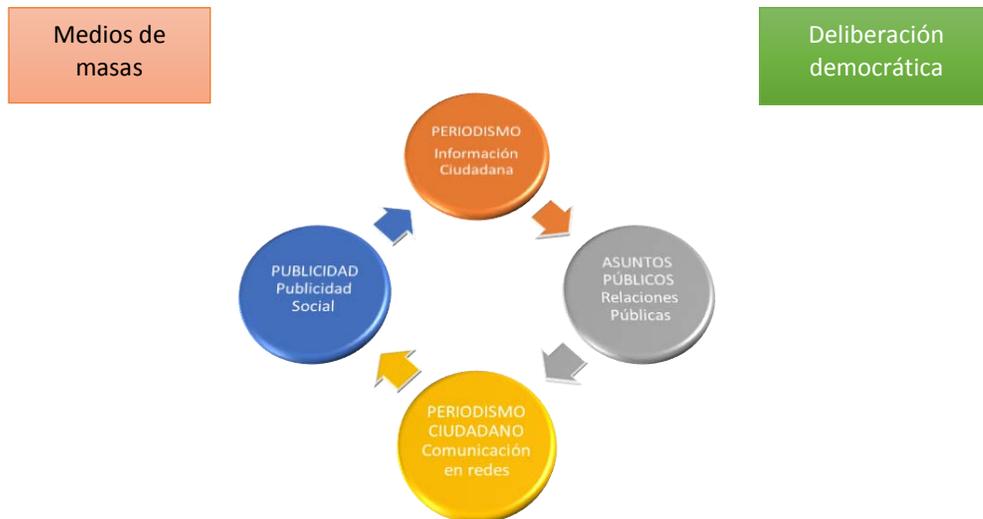
---

<sup>(66)</sup> José Ángel Cabrera y Nantzin Saldaña, 24 horas el Diario sin límites, **Peña Nieto promulga leyes telecom; anuncia Nueva cadena de TV pública**. [En línea]: <http://www.24-horas.mx/pena-nieto-promulga-leyes-telecom-anuncia-nueva-cadena-de-tv-publica/> [Consulta: 26. mar. 2015].

<sup>(67)</sup> DEMERS F. y LAVIGNE..., *op. cit.*, nota a pie (62), p.70.

democracia cuando funcionan como un espacio público y, por el otro, tienen también la misión de proteger la privacidad de la información que en ellos se vierte cuando es necesario.

El concepto de comunicación pública despertó la preocupación por el papel que desempeñan los medios, de tal forma que éstos pudieran funcionar como mecanismo que fusionara la opinión pública con la democracia. Demers y Lavigne presentan el siguiente gráfico:



(F5) Gráfico de los elementos que conforman la comunicación pública, relacionada con los medios de comunicación y la construcción de la democracia.

De acuerdo con el presente cuadro, el periodismo, publicidad, comunicación en redes y las relaciones públicas, con base en la información y contenido de los medios de masas provenientes de la deliberación democrática, convergen para dar espacio a los debates y asuntos públicos generados con base en la información ciudadana, la publicidad social, el periodismo ciudadano y temas relacionados con asuntos públicos. Los medios son un espacio público en la medida en la que dan cabida a la pluralidad. En este sentido, Monzón<sup>(68)</sup> se refiere al espacio público como el espacio creado por los medios de comunicación que se apoya en símbolos, códigos e imágenes que el receptor percibe como si fueran la realidad, es decir, los medios de comunicación y la labor de los periodistas sustituyen las limitaciones que tiene el hombre para percibir el mundo que los rodea. De esta manera, el espacio público desarrollado en los medios representa y reinterpreta la realidad bajo sus códigos de imagen y comunicación.

(F5) Diseño Diana Márquez Cisneros

(68) *Ídem*, nota a pie (65)

### 2.3. Políticas Públicas y Medios de Comunicación.

La participación ciudadana, de especialistas, académicos, profesionales, etcétera, y los medios de comunicación en el espacio público sirven para crear una agenda que puede conducir a la creación de políticas públicas. A pesar de que los políticos regularmente tienen su agenda hecha a partir de peticiones de la gente o temas que ellos mismos establecen, la participación de los medios puede modificarla o abrir nuevos caminos. Es poco probable que las organizaciones civiles o no gubernamentales incidan directamente en la construcción de las políticas públicas puesto que éstas dependen lógicamente del gobierno. Son pocas las agrupaciones que, al hacer público o dar a conocer mediante los medios de comunicación algún tema, pueden favorecer el intercambio de ideas, propiciar el debate público o la discusión, intrínsecos a la democracia.

En una interesante narración, Juan Francisco Escobedo <sup>(69)</sup> expuso la movilización del Grupo Oaxaca para crear la Ley Federal de Transparencia y Acceso a la Información. Este caso es particularmente interesante para este estudio porque el acceso a la información es el origen de la protección de datos en México y porque surgió a partir de la participación de la sociedad civil que logró abrir un espacio público para contribuir con el fortalecimiento de la democracia. Escobedo explica que, a pesar de décadas de persistencia autoritaria que atenuó la expresión de la opinión pública, constriñó las relaciones y el comportamiento de los medios y controló los temas de interés público, la sociedad civil y los movimientos políticos no menguaron por completo. Sólo unos grupos sociales fueron admitidos en las mediaciones gubernamentales, lo que hizo que la discusión y determinaciones de los temas e intercambios políticos desarrollados en el espacio público fueran predecibles, por lo que el debate democrático no existió. Las excepciones de esta política de control surgieron los movimientos sociales y de la sociedad civil y de la inconformidad en el seno de los órganos oficiales también aparecieron voces disonantes.

A pesar de que la Constitución tuvo reformas referentes al derecho a la información no hubo cambios significativos hasta entonces y peor todavía eran las Leyes de Imprenta y de Radio y Televisión, emblemáticas del autoritarismo que existía. Los cambios en estas relaciones obedecieron a modificaciones en las reglas informales, al intercambio de nuevos

---

<sup>(69)</sup> ESCOBEDO, Juan Francisco, *Movilización de opinión pública: El caso del Grupo Oaxaca y la Ley Federal de Transparencia y Acceso a la Información Pública, en México, UIA*, Revista Iberoamericana de Comunicación, núm. 3, otoño-invierno. 2002.

incentivos que alentaron un modelo de relaciones subordinadas, a la viabilidad y autonomía financiera de las Empresas mediáticas y a que disminuyó la capacidad del régimen para controlar los discursos y estadísticas electorales. Estos movimientos dieron oportunidad a otras voces, intereses y proyectos de la sociedad civil que fomentó la diversidad y fortaleció la opinión pública discursiva diferente de la opinión pública oficial. Ninguna fuerza política ni la llegada del Partido Acción Nacional (PAN) con Vicente Fox en el poder pudo oponerse a las movilizaciones que exigían mayor libertad de expresión y prensa para regular el derecho a la información, sino que, al contrario, sirvió para estimular la participación de voces en el espacio público. Fue dentro de este contexto que surgió el Grupo Oaxaca, abanderado del tema del derecho de acceso a la información pública en México, como lo comenta Escobedo. Este grupo surgió por la reflexión que ocurrió en el Seminario Nacional “Derecho a la Información y Reforma Democrática”, convocado por la Universidad Iberoamericana, la Fundación Información y Democracia, la Fundación Konrad Adenauer, El Universal, la Asociación de Editores de los Estados, la Asociación Mexicana de Editores y la Fraternidad de Reporteros de México en mayo de 2001, en Oaxaca, sin que tuviera la menor idea de los alcances que tendría hasta la fecha.

La movilización fue en un principio una iniciativa en la que participaron actores mediáticos, organizaciones no gubernamentales, periodistas y académicos. No se trató de un grupo articulado a partir de una convocatoria pública ni de una organización civil, sino que fue una mezcla de diferentes perfiles, profesionales, Empresarios, periodistas que buscaron orientación para gestionar la ley. De forma asombrosa, lograron convertir su propuesta en una iniciativa de ley en diciembre de 2001 con apoyo de las fracciones Partido Revolucionario Institucional (PRI), Partido de la Revolución Democrática (PRD), Partido Verde Ecologista de México (PVEM), Partido del Trabajo (PT) y Convergencia Democrática, que eran la oposición de la banca del PAN. Escobedo (2002) manifiesta que: “esta gestión política desde la sociedad civil constituye un hecho sin precedentes en la historia del régimen político autoritario”. La movilización de opinión pública y cabildeo del Grupo Oaxaca, junto con un despliegue de estrategias políticas, institucionales, sociales y mediáticas, hicieron posible alcanzar la aprobación de la Ley Federal de Acceso a la Información Pública que, aunque de forma accidental, fue también el inicio del derecho a la protección de datos en México.

Para comenzar, el Grupo Oaxaca escribió la Declaración de Oaxaca cuyo objetivo era impulsar la creación y aprobación de una Ley que se convirtió en un instrumento

mediático para incidir, posicionar al grupo en el espacio público y desplegar su capacidad para gestionar una temática que aclarara el espectro del derecho a la información, que hasta ese momento era muy confuso. Una vez que el grupo logró posicionar el tema, decidió enfocarse en la gestión y demanda pública al gobierno para que presentara una iniciativa de ley de acceso a la información pública sin que obtuvieran los resultados deseados porque la iniciativa gubernamental no ofreció los mínimos necesarios. Ante esta situación, el grupo inició una segunda fase. Escobedo menciona <sup>(70)</sup> que fue necesario adoptar otras medidas porque el gobierno entrante perdió su primer impulso y se comportó como el régimen priísta, con posiciones defensivas y poco claras sobre la iniciativa de ley que el mismo Presidente Fox había ofrecido en su campaña. Para evitar que el gobierno volviera a presentar una iniciativa de ley limitada, el Grupo Oaxaca volvió a reunirse nuevamente en Oaxaca para dar a conocer un Decálogo del Derecho a la Información que ubicó en la agenda pública los contenidos mínimos que debía abarcar el tema que los diarios El Universal y Reforma publicaron en primera plana. Esto dio un efecto político y mediático contundente porque le dio el liderazgo al Grupo Oaxaca en el tema y el gobierno apeló a la sociedad con foros de consulta pública, pero el Grupo no emitió su opinión en las consultas porque se dio cuenta de la estrategia del gobierno que pretendía minimizar sus actividades, tanto que incluso el Grupo Reforma publicó en un desplegado ¡No a la consulta del gobierno! y, a pesar de todos sus esfuerzos, la iniciativa del gobierno no prosperó.

Paralelo a estos acontecimientos, la comisión técnica del Grupo elaboró una iniciativa de ley que hizo llegar a los diputados porque es anticonstitucional que los ciudadanos presenten una iniciativa. Si los diputados y especialmente el gobierno hubieran ignorado la iniciativa habría sido totalmente incongruente, por lo que la estrategia del Grupo funcionó a la perfección, como lo describe Escobedo. El Ejecutivo, por su parte, también envió su propuesta de ley a la Cámara de Diputados, por lo que el Grupo Oaxaca tuvo que movilizarse para que su propuesta se convirtiera en una iniciativa formal y la comisión legislativa dictaminara a las dos simultáneamente. Aunque parecía difícil de lograr, el PRD, PT, PVEM y el único diputado de Convergencia la firmaron para presentarla el 6 de diciembre de 2001 ante el pleno de la Cámara. A partir de ese momento las decisiones estaban en manos del Congreso que dictaminó simultáneamente ambas leyes y abrió una mesa para la negociación entre representantes del gobierno y miembros del Grupo Oaxaca respaldados por los partidos opositores al PAN.

---

<sup>(70)</sup> *Ídem.*

A pesar de sus carencias, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, aprobada en abril de 2002, es muy valiosa porque fue el resultado de la participación ciudadana que inició el espacio público, junto con los medios de comunicación que fueron determinantes para crear una agenda pública y los partidos políticos de la oposición, que abrieron debate sobre un tema de interés social dentro del gobierno mismo para la construcción y fortalecimiento de la democracia, que es la finalidad de la comunicación pública. Este evento fue relevante en México porque en pocas ocasiones se ha visto de manera tan contundente el poder que puede tener la sociedad civil organizada y por el efecto colateral que tuvo para la aparición del derecho a la protección de datos personales.

Casos como estos crean sentido social porque abrir el espectro a la pluralidad permite la participación de diferentes opiniones que conducen a la democracia al haber un cambio en la forma de pensar y finalmente esto repercute en la creación de políticas públicas.

De acuerdo con Agrela <sup>(71)</sup> las políticas públicas son un instrumento central de los estados modernos que sirven para organizar a la sociedad. Clasifican y distinguen a la población, construyen a las personas como sujetos y objetos, regulan sus vidas y crean significados sobre diferentes grupos a los que están vinculados, opuestos o excluidos. Según lo señala Bordieu, citado por Agrela, los sistemas de clasificación producen efectos sociales, categorías que diferencian a unos de otros mediante políticas que otorgan diferentes roles y derechos como sujetos. Existen así categorías sociales, económicas, políticas, etcétera, con diversos significados. Menciona Agrela que las políticas públicas configuran un discurso institucionalizado que describe la realidad. Implican la elaboración de agendas políticas, definición de “problemáticas” referentes a colectivos concretos, elaboración e imposición de explicaciones y la oferta de soluciones que van implícitas en el planteamiento del problema mismo. Están relacionadas con la política y las decisiones de gobierno y la oposición, por lo que resultan útiles para aspectos como la discusión de la agenda pública, elecciones entre candidatos y programas, actividades de gobierno. Lahera <sup>(72)</sup> señala que gracias a las políticas públicas es posible acotar disposiciones políticas, diferenciar problemas y soluciones de manera específica, precisar diferencias, vincular los

---

<sup>(71)</sup> AGRELA ROMERO, Belén, *La acción social y las mujeres inmigrantes: ¿Hacia unos modelos de intervención?* [En línea] <<http://rabida.uhu.es/dspace/bitstream/handle/10272/170/b15124794.pdf?sequence=1> [Consulta 10. mar. 2015].

<sup>(72)</sup> LAHERA, Eugenio P., *Política y Políticas públicas*. [En línea] <<http://cgpp.app.jalisco.gob.mx/images/politicaspUBLICAS.pdf>. [Consulta 10. mar. 2015].

temas a soluciones más amplias o secuenciales, plantearse esfuerzos compartidos y participar de forma específica.

Una política pública de calidad responde a la acción y a la información unidos por un objetivo político definido democráticamente, desarrollados por el sector público, en ocasiones con la participación de la comunidad y del sector privado. Asimismo incluye orientaciones o contenidos, instrumentos o mecanismos, definiciones o modificaciones institucionales y los resultados esperados (Lahera).

Los elementos que deben considerar las políticas públicas son, de acuerdo con Lahera:<sup>(73)</sup>

1. Fundamentación amplia y no sólo específica (¿cuál es la idea?, ¿a dónde vamos?)
2. Estimación de costos y de alternativas de financiamiento
3. Factores para una evaluación de costo-beneficio social
4. Beneficio social marginal comparado con el de otras políticas (¿qué es prioritario?)
5. Consistencia interna y agregada (¿a qué se agrega? o ¿qué inicia?)
6. De apoyos y críticas probables (políticas, corporativas, académicas)
7. Oportunidad política
8. Lugar en la secuencia de medidas pertinentes (¿qué es primero?), (¿qué condiciona qué?)
9. Claridad de objetivos
10. Funcionalidad de los instrumentos
11. Indicadores (costo unitario, economía, eficacia, eficiencia)

Las políticas públicas, al igual que la comunicación pública, contribuyen con la construcción de la democracia y el bien común. En todas sus fases se complementan porque las políticas públicas hacen uso de las herramientas de otras disciplinas como Derecho, Economía, Comunicación, Sociología, Ingeniería, etcétera. En un tema como la protección de datos personales.

Como se ha comentado anteriormente, el desarrollo del derecho a la protección de datos en México proviene del derecho de acceso a la información pública que, a su vez, nació dentro de un espacio público. Por lo tanto, en nuestro país, las políticas públicas

---

<sup>(73)</sup> *Ídem.*

emergentes en torno a los datos personales no lograron desprenderse totalmente del acceso a la información y son garantizadas por el mismo órgano institucional. Dado que desde un principio la aparición de la protección de datos personales no fue un evento esperado no se puede hablar de políticas públicas planeadas específicamente con este fin sino que las acciones a seguir fueron elaboradas en función a las necesidades que surgieron a partir del derecho de acceso a la información, puesto que ni siquiera estaba definido como un derecho independiente sino que poco a poco fue cobrando autonomía.

Por lo tanto, las políticas públicas de protección de datos personales que comenzaron a crearse, como se ha visto en el desarrollo de la investigación, fueron en función del sector público puesto que el derecho de acceso a la información pertenece a este ámbito, desde donde inició la protección de los datos personales como su límite.

Entre las principales políticas públicas que figuran se encuentran:

- La creación de un órgano garante del derecho a la protección de los datos personales, el IFAI, que poco a poco vislumbró la necesidad de establecer lineamientos que complementarían la Ley y que se ha encargado de extender el derecho hacia el sector privado.
- Ley Federal de Transparencia y Acceso a la Información Pública y su reglamento.
- Lineamientos que deben observar las dependencias y entidades públicas con respecto a los datos personales.
- Lineamientos que deben seguir las dependencias públicas federales para responder a las solicitudes de acceso a datos personales que formulen los particulares.
- Lineamientos con los que las dependencias públicas federales notifican al IFAI las listas de sus sistemas de datos personales.
- Lineamientos de protección de datos personales y la creación del Sistema Persona, mediante el cual las personas pueden ejercer electrónicamente su derecho a la autodeterminación informativa.

Todas estas políticas públicas creadas en torno a la protección de los datos personales resultaban todavía insuficientes puesto que había retos que superar, como lograr que fuera un derecho autónomo. Esto se alcanzó con las posteriores reformas

constitucionales que, además, dotaron al congreso con poder para legislar sobre los datos personales en posesión de particulares, cuyo fruto de estas acciones fue la Ley de Protección de Datos Personales en Posesión de Particulares, así como la próxima aprobación de la reforma, que eleva la protección de datos personales del sector público a un mismo nivel que el sector privado, a pesar de las diferencias de opiniones al respecto por tratarse de dos leyes para un mismo tema.

Asimismo, ante el vacío legislativo que existía en la materia, diferentes sectores establecían la protección de datos personales con leyes sectoriales, reglamentos, normas, códigos de ética, etcétera, mencionados en los capítulos dos y tres, que llenaban el vacío constitucional existente para proteger la información personal y actualmente sirven para complementar la actividad desarrollada por el IFAI, todo esto sin dejar de lado los foros que han contribuido con el aprendizaje, difusión, enriquecimiento y cooperación para la práctica y aplicación del derecho. De la misma manera, algunas instituciones privadas contaban con políticas internas para proteger la confidencialidad de la información que poseen y sobre el tratamiento de datos.

Los propósitos de todas estas directrices en las políticas públicas, para resumir, han sido:

- Promover una cultura de seguridad de los datos personales entre todos los involucrados en el tratamiento de la información así como de los propietarios mismos para proteger su integridad física.
- Crear conciencia sobre los riesgos que representa un mal uso de los datos personales.
- Difundir las políticas establecidas, prácticas, medidas y procedimientos disponibles para atenuar dichos riesgos.
- Integrar un cuerpo legislativo y referencial para que el derecho a la protección de datos pueda ser comprendido y adoptado para la ejecución de las políticas establecidas.
- Fomentar un mejor conocimiento del derecho.
- Crear estrategias para proteger la vida íntima y privada de las personas, contenida en los datos personales, así como su justo balance para determinar cuáles son sus excepciones.

- Incentivar la autoprotección de los titulares de los datos y mecanismos de autorregulación por parte de las Empresas en el sector privado.
- Colocar a México en un nivel de competencia para que pueda intercambiar información con otros países bajo estándares de seguridad establecidos internacionalmente con el fin de incrementar, a su vez, su desarrollo comercial.
- Crear normas o sellos de calidad que las Empresas puedan adquirir para garantizar su responsabilidad hacia la información personal que poseen.

De manera general, es de señalarse que las políticas públicas establecidas deben fortalecer los derechos ARCO, buscar la capacitación para la protección de datos personales y en general de los derechos humanos, lo que abarca tanto la capacitación de los funcionarios como el fomento de una cultura de educación para la autoprotección.

Los resultados de la aplicación de las políticas establecidas se vislumbran al paso del tiempo desde la aparición del concepto mismo de la protección de datos personales en la LAI. Con aciertos y errores, las políticas públicas creadas en torno a este derecho han dado pasos que lo afirman como tal dentro del Derecho Mexicano. Sin embargo, su difusión es indispensable porque se trata de un tema bastante nuevo en México que debe consolidarse para su correcta aplicación.

#### **2.4. La protección de datos personales en los medios de comunicación.**

Los datos personales en los medios de comunicación podrían ser utilizados para atacar personas y afectar su imagen, con daños irreparables a la misma, sobre todo cuando son acusaciones falsas y de mala fe, por esto cabría preguntar si corresponde a alguna instancia, como el IFAI, salvaguardar la vida privada de las personas y establecer políticas públicas respecto al tema.

En este sentido, en lo que concierne a los derechos al honor y a la privacidad de personas públicas, los ordenamientos jurídicos cuentan con un abanico legal o jurisprudencialmente asentado sobre qué es y qué no es un equilibrio entre estos dos derechos. La Jurisprudencia mexicana ha dictaminado en algunos casos sobre este tema para esclarecer que cuando se trata de la actividad informativa de los medios, éstos se verán guiados por la ética periodística sustentados en su libertad de expresión. Entre algunos ejemplos de la jurisprudencia es posible mencionar los siguientes:

Una regla ampliamente revisada en el derecho comparado señala que quienes desempeñan, han desempeñado o desean desempeñar responsabilidades públicas tienen menos oposición normativa general que los ciudadanos comunes en términos de intimidad y respeto al honor, frente a actuaciones en los medios de comunicación. Esto es debido a la actividad que desempeñan, que implica una observación constante de su persona. En lo que se refiere a la intimidad, la difusión y conocimiento de datos en ocasiones puede ser de interés público porque, a pesar de que se trate de datos privados desde alguna perspectiva, guardan conexión con asuntos que la ciudadanía debe conocer para valorar su desempeño como servidores o titulares de cargos públicos, lo que naturalmente conlleva mayor afectación a su privacidad. (Tesis aislada 165820, 2009).<sup>(74)</sup>

La tesis aislada con registro no. 172912 (2007)<sup>(75)</sup> habla sobre la responsabilidad de periodistas y medios de comunicación. La actividad periodística requiere armonía entre el derecho a la libertad de expresión y los principios fundamentales del hombre y su dignidad. Esta armonía haya lugar en el principio universal de la veracidad, lo que representa que los hechos transmitidos por el informador deben ser veraces, basados en datos objetivos para no defraudar el derecho social a la información. La Constitución mexicana no tutela conductas negligentes, ni menos a quien comunique como hechos, simples rumores, invenciones o insinuaciones insidiosas, únicamente ampara información rectamente obtenida y difundida, aun cuando sea controvertible.

De manera adicional, la tesis aislada con registro no. 164987 (2010)<sup>(76)</sup> pareciera que deslinda al comunicador de toda responsabilidad de cuidar la calidad de la información dada por terceros puesto que se trata de su opinión personal. Menciona el “reportaje neutral”, en el que el medio de comunicación debe limitarse a transcribir o difundir lo dicho o declarado por un tercero, por lo que quien diga las declaraciones reproducidas por el medio es su autor material. Para saber si en un caso concreto se está ante un reportaje neutral y si la afectación a la privacidad de una persona es legítima, deben existir dos requisitos: la veracidad, que contiene la certeza de que la declaración corresponde a un tercero, y la relevancia pública de lo informado. Por esto, esta jurisprudencia declara que cuando los comunicadores únicamente publican o divulgan información de la autoría de terceros, no

---

<sup>(74)</sup> Tesis aislada No. 165820. Derechos al honor y a la privacidad. 1a. CCXIX/2009 Primera Sala. Novena Época. Semanario Judicial de la Federación y su Gaceta. Tomo CCXIX/2009, Diciembre de 2009, Pág. 278.

<sup>(75)</sup> Tesis aislada No. 172912. Responsabilidad de periodistas y medios de comunicación. I.3o.C.607 C. Primera Sala. Novena Época. Semanario Judicial de la Federación y su Gaceta. Tomo XXV, Marzo de 2007, Pág. 278.

<sup>(76)</sup> Tesis aislada No. 164987. Medios de comunicación. 1a. XLV/2010. Primera Sala. Novena Época. Semanario Judicial de la Federación y su Gaceta. Tomo XXXI, Marzo de 2010, Pág. 929

están en la obligación verificar o calificar la relevancia que pudiera tener sobre la reputación o el honor de una persona por la intromisión en su intimidad, o si sus aseveraciones tienen relevancia pública o no y, además, si son legítimas, porque entonces requeriría repartir responsabilidades entre los que comunican la información, y eso restringiría la libertad de expresión y el derecho a la información, que tienen una dimensión individual y social porque no sólo exige que no se impida la posibilidad del individuo de manifestarse libremente sino que también demanda conocer la expresión del pensamiento ajeno. Por esta razón, un reportaje neutral protege al comunicador en su posibilidad de expresar y publicar sus ideas, opiniones e información de un tercero libremente, dentro del régimen democrático.

Por su parte, una consulta realizada a la Fundación para la Libertad de la Expresión<sup>(77)</sup> sobre la libertad de expresión y su límite, responde que:

Hay que distinguir entre la conducta ética y la legal. En el caso de los supuestos jurídicos existe un elemento diferenciador del derecho que es la coercibilidad (que obliga a cumplir con la consecuencia aún en contra de nuestra voluntad), en cambio la conducta ética se plasma en la actuación voluntaria en función del valor que tiene inmersa esa conducta. Como todo derecho el de la libertad de expresión encuentra su límite en el derecho de los demás que en este caso es principalmente la vida privada, el honor y la propia imagen. La ética es un mecanismo de autorregulación del propio medio y/o periodista, es un llamado a la decencia y prudencia en el manejo de la información y la opinión.

La libertad no lo hace a uno antiético si la armonizamos con el ejercicio de los derechos de los demás. La máxima "no hagas lo que no quieras que te hagan" cobra sentido en una sociedad en donde no sólo la norma jurídica nos regula. El ejercicio ético de la libertad de expresión se convierte en una coraza de credibilidad y legitimación que hace que la sociedad reaccione cuando ese medio y/o periodista es atacado injustamente por el ejercicio responsable de la libertad de expresión. Sin embargo, el crear códigos éticos que no se cumplen se convierte en una simulación y farsa si no se toman en serio en el uso responsable de la libertad y el deber de informar.

Existen temas que representan especial dificultad para los periodistas para decidir si deben publicar o no datos personales que hagan identificable al sujeto de su noticia. Tales temas pueden girar en torno a violaciones, crímenes, menores de edad, suicidios, asesinatos, asaltos, etcétera. Por esto, la duda de cuándo un periodista puede invadir la

---

<sup>(77)</sup> Fundación para la Libertad de Expresión. Consulta No. 17. Preguntas frecuentes. Consulta: 20. marzo. 2015. En línea <http://www.fundalex.org/preguntas-frecuentes-3.php>.

privacidad de las personas se resuelve más desde la vía ética que de la legal, de acuerdo con lo establecido por el código de ética de cada medio y sus propias políticas. Sin embargo, la ética periodística no debería ser el único recurso al que se encomiende la seguridad de los datos personales puesto que puede ser aplicada a conveniencia o interés de cada medio.

Luz González <sup>(78)</sup>, periodista de El Universal, explica que: “El asunto es complicado porque no hay regulaciones específicas, salvo el tema del secreto profesional, y queda a criterio del periodista y del medio. En general, existen reglas no escritas, como no publicar el nombre de tus fuentes si ellos lo solicitan, pero hay medios que tienen como norma no publicar notas sin fuentes, entonces por lo menos el editor o el jefe de información deben conocer el origen de la información y en función de ello valorar si la publican. Eso es parte del Código de Ética de El Universal, por ejemplo”.

González comenta que un caso reciente en el que se aprecian las diferencias es en la masacre de los 72 migrantes que ocurrió en Tamaulipas. Reforma y otros medios publicaron el nombre y la fotografía del sobreviviente pese a que ello representaba un riesgo para su vida. En otras ocasiones Reforma ha publicado la identidad real de testigos protegidos en los casos de delincuencia organizada y hasta hace poco medios impresos y electrónicos (televisoras) publicaban el nombre y rostro de menores detenidos en operativos policiales. Luz González expresa hay mucho por hacer en este ámbito, pero personalmente protege siempre la identidad de víctimas del delito, menores, testigos protegidos y de todo el que se lo solicite, a pesar de que a veces eso frena la publicación de las investigaciones, pero es un tema de ética y de principios.

Por otra parte, no resulta menos complejo cuando se trata de personas no públicas. Desde la ética periodística no deberían publicarse las víctimas de accidentes o percances, pero los medios publican imágenes de las víctimas porque argumentan que se trata de información. En ese sentido, un verdadero comunicador no debería transmitir la nota roja ni fomentar el amarillismo. En caso de que surja algún tema de mucho interés con respecto a una muerte, violación o algo similar únicamente podría comentarse el incidente pero para hacer un llamado a la reflexión y cuestionar qué hemos hecho como sociedad para llegar a esa condición porque, afirma, posiblemente no hay respuestas pero sí las preguntas, y eso mismo incide en las formas de pensamiento. Existen, por otra parte, códigos de ética compartidos por los medios de comunicación que orientan el trabajo de los periodistas, así

---

<sup>(78)</sup> *Íbidem*, nota a pie (46).

como acuerdos internacionales, por ejemplo si hay alguna víctima de un accidente no se difunde la información hasta que se sabe que la familia ya está enterada del accidente o asesinato. Sin embargo, con las nuevas tecnologías esto ya es muy difícil de controlar puesto que ahora no sólo se publican en el periódico sino también en Internet o en las redes sociales, por lo que es muy difícil preservar la vida privada.

Respecto de leyes más específicas, González considera que es necesario que se establezcan políticas con toda precisión, que los medios de comunicación y las autoridades deben quedar obligados a garantizar esa protección, con sanciones en caso de no acatarlas, y, a diferencia de Troncoso, opina que el cumplimiento de esa obligación debe estar vigilado por el IFAI, la Comisión Nacional de Derechos Humanos (en adelante CNDH) y las comisiones estatales de derechos humanos, organismos que deberían establecer políticas públicas al respecto. Ante tal situación, los medios de comunicación deben tener como uno de sus principales principios, la protección de los datos personales o información estrictamente de carácter personal o familiar.

Dentro de las posturas que señalan los códigos deontológicos relativos a la protección de la intimidad personal, refieren que se deben evitar las intromisiones ilegítimas a la esfera íntima de las personas, así como también salvaguardar el derecho a la propia imagen, es decir, la reproducción total o parcial de una persona en particular

No obstante lo anterior, el creciente uso de las nuevas tecnologías de la información, como lo es Internet, ha alterado considerablemente los aspectos deontológicos ya que es común ver en dicho medio, información poco confiable, en otros casos anónima, alterada y tendenciosa lo que genera que se cuestione en alto grado la veracidad del informante debido a que no existen normas de control y sea reciente la incorporación de mecanismos de seguimiento, seguridad y vigilancia de los contenidos.

Ha sido, de manera paulatina, como han ido modificándose los códigos deontológicos para adaptarse a la problemática, a las necesidades actuales y a los espacios informáticos que van surgiendo. Por ello, algunos medios de comunicación nacionales e internacionales, de manera individual o bien a través de sus asociaciones o redes de periodistas, han plasmado de manera general las directrices a las cuales deben apegarse sus miembros o en lo general, los periodistas.

Dichos códigos éticos, abarcan principios como la confianza pública, la verdad, la justicia, la integridad, el respeto, entre otros; pero sólo se observa en lo general, un breve apartado en el que deben velar por no vulnerar la integridad, la seguridad y la imagen de las personas, es decir, ser cautelosos con la difusión de los datos personales y la esfera de la vida privada.

Asimismo, estos códigos deontológicos van acompañados por normativas específicas que de este modo aseguran un debido tratamiento a los derechos que todo periodista debe observar en el ejercicio de su profesión. Cabe señalar que aunado a lo anterior, ante la creciente necesidad de salvaguardar el derecho a la protección de los datos personales, han comenzado a surgir diversas leyes en la materia en algunas partes del país, así como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

## **2.5. Los Datos personales en las Organizaciones y las Políticas de Comunicación Internas.**

Cabe recordar que la comunicación pública también surge dentro de las instituciones privadas sobre temas que conciernen a la colectividad. El tema de la protección de datos personales atañe tanto a directivos, empleados, usuarios y titulares de la información, por lo tanto, debe ser un tema vital para las Empresas tener políticas internas referentes a la seguridad de los datos.

Las políticas de comunicación internas de las Empresas y organizaciones están directamente relacionadas con sus mecanismos de autorregulación. En México la mayoría de las Empresas son PyMES que no necesariamente cuentan con este tipo de políticas para proteger la información personal, aunque a partir de la nueva ley no van a poder darse el lujo de no implementarlas.

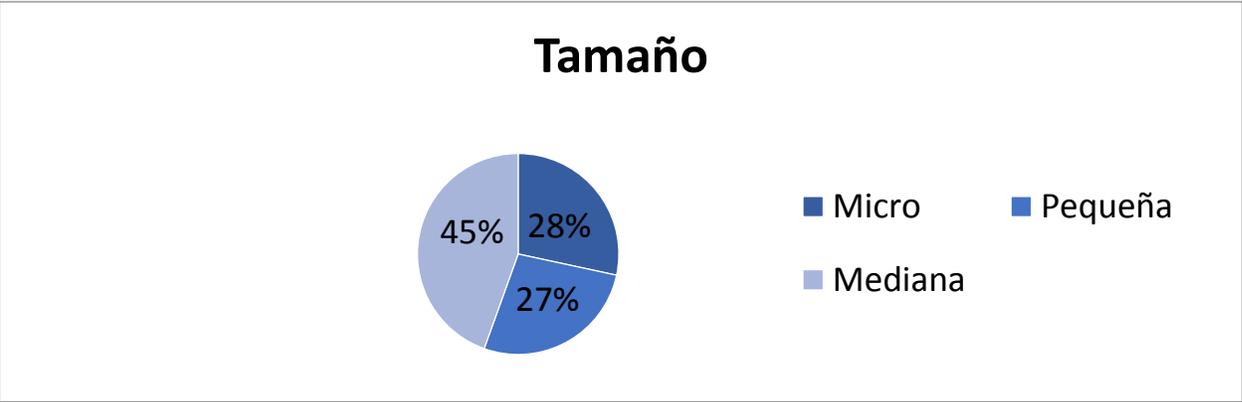
En la actualidad uno de los principales retos que enfrentan las Empresas en nuestro país es la baja cultura de privacidad y por tanto la Protección de Datos Personales; sin embargo, considero que este tema no debería ser sólo de interés para estas organizaciones sino para cada una de las personas, ya que como bien es sabido, los derechos humanos se presentan como exigencias morales de realización, tanto a nivel personal como comunitario y que, a partir del desarrollo histórico se encuentran sustentados por un aparato institucional amplio así como de un cuerpo normativo en continua expansión.

En este marco, los principales exponentes de esta idea Jose Luis Piñar Mañas y Lina Ornelas Núñez <sup>(79)</sup>, consideran que introducir la variable tecnológica significa atender a la necesidad de traducir el discurso de los derechos humanos en términos que puedan abarcar también a la ciencia y la tecnología, en virtud de que éstos son elementos que modifican el concepto de espacio o ámbito en el que se manifiestan, profundizan y desarrollan los derechos humanos en lo general. De tal forma que, este nuevo contexto abre nuevas perspectivas para comprender, de una forma más amplia la Declaración Universal de los Derechos Humanos, al surgir problemas éticos, políticos y jurídicos que tienen que ver con nuestros derechos.

Un hecho que confirma este desconocimiento con referencia a políticas internas de protección de datos personales fue corroborado por la Secretaría de Economía quien realizó una encuesta en línea enfocada a MiPYMES. <sup>(80)</sup>.

El periodo sobre el que se reportan las respuestas comprende del 2 de febrero al 23 de febrero de 2013. Se establecieron sólo 9 reactivos con respuestas cerradas para facilitar el llenado y envío de información.

Se recibieron las respuestas de 155 Empresas.

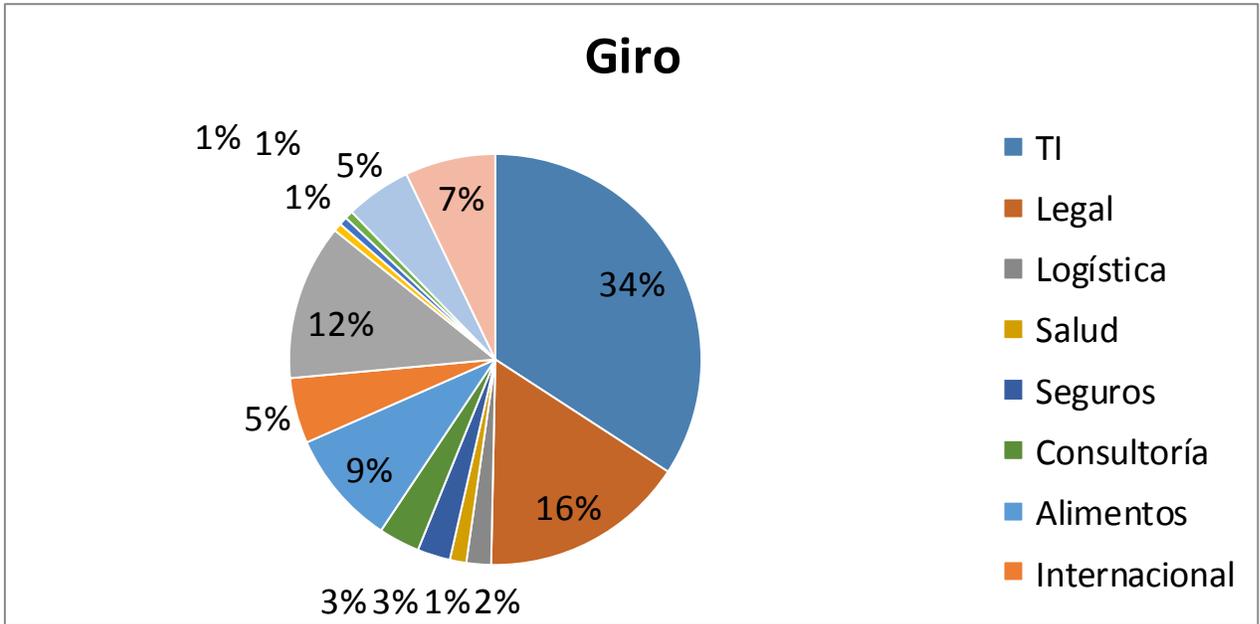


<sup>(F6)</sup> Fuente: FMI, INEGI, SECRETARIA DE ECONOMÍA

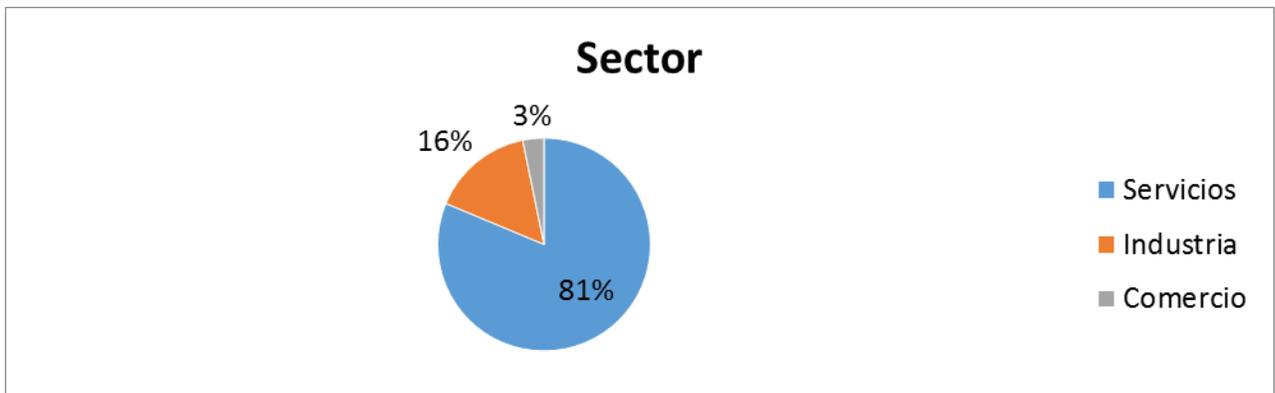
<sup>(79)</sup> PIÑAR, José Luis y ORNELAS, Lina, *La Protección de Datos Personales en México*, México, D.F., Ed., Tirant Lo Blanch México, 2013, p.21.

<sup>(80)</sup> Fuente: FMI, INEGI, Secretaría de Economía

<sup>(F6)</sup> Diseño Diana Márquez Cisneros



(F7) Fuente: FMI, INEGI, SECRETARÍA DE ECONOMÍA



(F8) Fuente: FMI, INEGI, SECRETARÍA DE ECONOMÍA

## 2.6. Aspectos generales.

La comunicación, el espacio público, los medios de comunicación y la participación ciudadana, fueron elementos claves para que en México surgiera, aunque de forma indirecta el derecho a la protección de datos personales. Aunque todavía falta camino por recorrer para su debida aplicación, nuestro país está abierto a la creación de políticas públicas que defienden estos derechos de tercera generación correspondientes a las democracias modernas, y que además no es un tema que se infiltra únicamente en el ámbito gubernamental, sino en el ámbito privado.

(F7) Diseño Diana Márquez Cisneros

(F8) Diseño Diana Márquez Cisneros

## CAPÍTULO TERCERO

### ASPECTOS JURÍDICOS DE SEGURIDAD DE LA INFORMACIÓN: MEDIDAS DE CUMPLIMIENTO EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN EL SECTOR EMPRESARIAL

#### 3.1. Tecnología y Derecho: Un paso al mundo jurídico virtual.

Globalización, Neoliberalismo, Cibernética, Robótica, Genética, Internet, Realidad Virtual entre otros términos, han tomado gran interés en un número siempre creciente de personas (científicos, académicos, intelectuales, empleados, obreros y en especial, en el de los jóvenes). Estos vocablos como fenómenos y producto de la revolución tecnológica y científica, han producido cambios significantes en las relaciones mutuas entre individuos y naciones por igual; cambios que a simple vista son de gran beneficio para la humanidad, sea en el campo de la educación, en el mundo Empresarial, en la investigación científica e incluso tecnológica, así como en las comunicaciones casi instantáneas como es el caso de nuestro objeto de estudio, y mucho más.

Sin embargo, al mismo tiempo que como sociedad hemos sabido aprovechar lo mejor del desarrollo cultural, a la par han apareciendo una serie de elementos negativos; un preocupante crecimiento de la pobreza, un egoísmo destructivo de los valores sociales tradicionales de la familia y la sociedad, una concentración de poder económico y político en manos de pocos con la resultante exclusión de participación real de las mayorías y aunque no somos indolentes a todos estos aspectos, y consideramos que cada uno de ellos merece un estudio por separado, a nosotros solo nos interesan las consecuencias jurídicas derivadas del uso de las denominadas **nuevas tecnologías**.

Dedicaré los esfuerzos al estudio y análisis de las instituciones jurídicas que conocemos, cuáles deben ser los resultados de su evolución y la manera en la que coexisten, vamos a estudiar cuales son los principales problemas derivados del uso de las nuevas tecnologías y que para el campo de las Ciencias Jurídicas tienen relevancia, analizaremos también, si nuestro Derecho está preparado para afrontar con éxito el llamado **shock del futuro** <sup>(81)</sup>; criticare los nuevos conceptos jurídicos que se han incorporado a la

---

<sup>(81)</sup> En 1965, en un artículo publicado en el periódico *Horizon*, Alvin Toffler inventó el término "shock del futuro" para designar la desastrosa tensión y desorientación que se provoca en los individuos al obligarles a un cambio excesivo en un lapso de tiempo demasiado breve, en ese sentido, no planteó el término como la palabra definitiva, sino que al igual que nosotros solo pretendió esbozar una primera aproximación a las nuevas realidades, llenas de peligros y de promesas, creadas por el impulso acelerador de la tecnología.

legislación mexicana y del mundo en general, con motivo del uso de la tecnología, para finalmente hacer algunas anotaciones con respecto a las necesidad de incorporar nuevos elementos a las doctrinas clásicas de instituciones legales bien definidas como las de las obligaciones y en especial a la protección de datos personales.

El Ciberespacio es una realidad producida por la sociedad; un entorno electrónico creado por un sistema de redes computacionales, que puede ser utilizado por los individuos para su exploración <sup>(82)</sup>. Este concepto surge en referencia a un mundo utópico e irreal, el cual el autor de la novela “Neuromancer” <sup>(83)</sup> probablemente no imaginó que llegara a existir. Nos encontramos ante un mundo basado en redes de computadoras, por las cuales fluye constantemente información, textos, sonidos y en sí, datos que se transmiten en pocos segundos y que eliminan las barreras geográficas y jurídicas existentes en el mundo material.

Como lo mencione a lo largo de la presente investigación, el Internet constituye un medio de comunicación muy extendido en el ámbito de las relaciones entre particulares, en la medida en que se ahorra tiempo y dinero. De acuerdo a una investigación hecha por *Cysco Systems*, para Latinoamérica, solamente en 1998, el servicio de correos de EE.UU entregó 10,000 millones de cartas; mientras que el número de mensajes e-mail, en el mismo año, ascendió a una cifra entre 618,000 millones y 4 billones <sup>(84)</sup>; a lo que se suma el aumento desproporcional en el número de usuarios que utilizan cada día con más frecuencia las **nuevas tecnologías**.

Puede decirse que acorde a nuestro primordial objeto de estudio, la consecuencia del aumento de los usuarios de las redes informáticas y de los demás medios de telecomunicación, trae como resultado, un incremento en el tráfico de la información que circula diariamente por los sistemas computacionales del mundo entero y con ello **una serie de problemáticas jurídicas que requieren de solución; y es por ello que se hace preciso el análisis de la información transfronteriza que se usa como base para crear esta nueva clase de obligaciones y que se encuentra circunscrita al marco de la evolución del comercio internacional, así como a la transición del mercado material al espacio digital.**

---

<sup>(82)</sup> PFAFFENBERGER, Bryan, *Internet in plain english*, New York, Estados Unidos, Edit., MIS Press, 1994, p. 112.

<sup>(83)</sup> “Neuromancer” es el título de una novela de ciencia-ficción de William Gibson la cual define al ciberespacio de una futura red computacional, como una “alucinación colectiva” basada en un mundo utópico.

<sup>(84)</sup> Cisco Systems Inc. Datos principales [En línea] Latinoamerica <[http://www.cisco.com/global/LA/LATAM/cs/ic/de/datos\\_principales.shtml](http://www.cisco.com/global/LA/LATAM/cs/ic/de/datos_principales.shtml)> [Consulta: 28. mar. 2015].

Gracias a las telecomunicaciones, las transacciones comerciales, a las oportunidades de negocio así como la contratación electrónica, se hace cada vez más asequible la información, por ello los usuarios de los servicios de información requieren de más y más seguridad tecnológica y jurídica, ésta, según se afirmó (*supra*, 1.9 y 1.10) se debe instituir porque posee su propio campo de estudio, sistematización, autonomía y principios; y toda vez que el problema de la **seguridad transaccional en línea** es en parte tecnológico y en parte jurídico, sólo la alianza entre ambos, será el vehículo que haga de las transacciones jurídicas en línea un medio seguro de celebrar toda clase de actos jurídicos, aunque en este análisis se constriña al mundo del Derecho Civil y Mercantil.

### **3.2. Problemas jurídicos derivados de las comunicaciones en línea.**

Gracias a las **nuevas tecnologías**, el intercambio de información entre los usuarios conectados a las redes computacionales, se hace más rápida, eficiente y continua, generando una serie de relaciones tanto personales como jurídicas que requieren de la protección jurídica.

Podemos decir que el tráfico de información, son una consecuencia lógica, producto de la utilización de las **comunicaciones en línea**, y aunque este fenómeno ya se había visto antes con la invención de otros medios como pueden ser el teléfono o el telégrafo, nunca antes tuvo el auge que tiene en nuestros días, lo que hace cada vez más necesario el estudio de las implicaciones jurídicas y sociológicas que tiene la utilización de la tecnología en el ámbito de las comunicaciones y en el de las relaciones jurídicas, comerciales y/o Empresariales. La utilización de los medios tecnológicos al momento de intercambiar información genera una amplia gama de problemas, pero éstos se acentúan cuando la información que se intercambia nos lleva a la celebración de actos jurídicos que representan nuevas complicaciones para las potestades jurisdiccionales de los Estados, en donde muchas veces se confunden con las obligaciones tradicionales.

Uno de los principales problemas que enfrentan las transacciones en línea, es sin duda el Flujo de Datos Transfronterizos (en adelante FDT), que sigue provocando preocupación a nivel internacional en función de su trascendencia tan significativos, y puede afirmarse, que éste ha tenido dos efectos, por un lado ha desencadenado una serie de consecuencias positivas pero también otras que han sido negativas, como ocurre con cualquier avance científico. En efecto, se está considerando que este flujo de información

(FDT) <sup>(85)</sup> aporta beneficios considerables a las colectividades nacionales, sin embargo también representa una serie de riesgos que no pueden ser dejados de lado, por la problemática jurídica que trae consigo y que se detallan en seguida.

Actualmente Internet no suele considerarse un entorno seguro, al menos no para desarrolladores de sistemas, especialistas en seguridad de redes y por supuesto para los juristas modernos, y es que la mayor de las ventajas de la Red, es también su mayor problema, ya que terceros **no autorizados** podrían acceder a los datos que envían a diario las Empresas a través de la Red, lo que podría conducir a la revelación de la información más confidencial de sus actividades, cambios en su contenido o fallos técnicos, aun cuando emisor y receptor se encuentren en un mismo país, o bien, que rebasando fronteras la información que una Empresa o persona envía a través del Internet puede arribar a otro territorio al que no estaba destinada, en el que sin duda existe un nivel de **protección de datos** inferior al existente en el país del emisor original, circunstancia que dejaría al usuario promedio en un claro estado de incertidumbre jurídica.

En nuestro país el artículo 16 de la Constitución General de la República garantiza el derecho de los gobernados a la intimidad, al señalar claramente que nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. Sería absurdo considerar que esta prerrogativa que protege la intimidad de los gobernados no se extiende a la información que se transmite a través de las redes computacionales en materia de datos personales.

En ese sentido la Constitución española es mucho más explícita al señalar en su artículo 18,4 que el legislador deberá limitar el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos y el legítimo ejercicio de sus derechos. Como vemos, la aún joven Constitución del país europeo (1978), le permitió expresamente la articulación de garantías contra la posible utilización anticonstitucional e ilegal de ese fenómeno de la contemporaneidad al que hemos llamado **Alta Tecnología** (permítaseme resaltarla así). Como es de observarse, en algunos países de Europa, ya se está previendo que las personas puedan hacer mal uso de la información personal que los individuos van dejando a través del Internet, como son los nombres, las direcciones, los números de seguro social o los de las tarjetas de crédito; pero no solo las personas físicas, sino también las

---

<sup>(85)</sup> TÉLLEZ-VALDÉS, Julio, **Derecho informático**, México, ed., Mc Graw-Hill, 2ª ed, 2000, p. 77.

personas jurídico-colectivas pueden ser víctimas de estos atropellos, ya que la Información que circula a través de Internet o las propias redes internas de las Empresas (intranets), pueden ser motivo de ilícitos, ya sea como medios o como objetivos, por lo que la existencia de una regulación internacional en términos penales limitaría dichas acciones, ya no en forma exclusivamente correctiva sino también preventiva.

El problema real, es que el envío de información a otro país en el estado actual del Derecho, permite que los emisores escapen a la reglamentación a que eventualmente pudieran estar sometidos en función del país de origen y de allí que se puedan derivar atentados graves a las garantías de los ciudadanos o aun a la seguridad de los Estados, lo cual amerita, sin duda, una solución jurídica.

### **3.3. La conciencia de riesgo en el sector Empresarial.**

Son muchos los retos a los que se enfrentan tanto las Empresas como las personas en cuanto al uso de la tecnología, e incluso las propias Tecnologías de la Información y la Comunicación (TIC), son la razón por la cual en diversos países inició la preocupación por regular estos aspectos. Esto es, la tecnología que cada vez más proliferaba en los años ochenta y que supuso inclusive que se desarrollaran muchos análisis teóricos para analizar los fenómenos que planteaba ésta, desde el punto de vista sociológico o comunicacional, también admitió estudios y enmiendas en el plano jurídico, toda vez que se consideraba el potencial que podría tener de vulnerar las esferas de derechos humanos ya protegidos, como el de la intimidad y el del honor y la propia imagen.

La conciencia de riesgo es baja en nuestro país, siempre se piensa que lo malo puede ocurrirle a alguien más, no a uno mismo, si a esto le sumamos la aparente intangibilidad y la inherente complejidad de los riesgos asociados a un inadecuado manejo o tratamiento de datos, esta conciencia tiende a ser aún menor. El sector Empresarial de nuestro país muestra incredulidad ante la obligación de atender el cumplimiento de algunas regulaciones, los medios de comunicación consignaron que, casi un año después de que la LFPDPPP entrara en vigor, prácticamente el 50% de las organizaciones no la conocían. <sup>(86)</sup>

Es de explorado Derecho que el desánimo en el cumplimiento se debe al destino final que algunas leyes han tenido en México, sin embargo, la atención a una ley que promueve la protección de datos personales es positiva para todos. Es por ello, que como ciudadanos

---

<sup>(86)</sup> *Íbidem*, nota a pie (51), p. 315.

comprendamos con claridad los beneficios que su cumplimiento nos confiere, sólo así será posible que entendamos las responsabilidades que, como especialistas en derecho Empresarial y como ejecutivos de las organizaciones privadas, tenemos al tratar los datos personales de quien nos los confía para un fin específico. Ya que como bien es sabido, en muchos de los casos el enemigo más peligroso está en casa y esto se debe a la falta de conocimiento e iniciativas personales, sin identificar los peligros que se invocan cuando actuamos aparentemente en pro de las Empresas. La mayoría de los fraudes han sido cometidos por empleados internos de la Empresa, por lo que es necesario mantener un control estricto sobre quién y de qué forma se manejan los bancos de datos. Crear Conciencia en el personal sobre la importancia y riesgo del manejo de datos personales en la labor de cada uno de los que laboran dentro de la Empresa y también afuera como titulares, a fin de lograr tener una cultura de protección de datos personales y prevenir cualquier inconveniente. Debiendo establecer ésta cultura de protección de datos personales como un principio general en las Empresas.

#### **3.4. Elementos necesarios para la existencia de las obligaciones en línea.**

Podemos afirmar que el cumplimiento de las condiciones que darían lugar a la existencia de una obligación válida en una jurisdicción concreta, no implica su necesario cumplimiento en otra, o que dos jurisdicciones lleguen siquiera a compartir las mismas condiciones, por lo que a los elementos básicos de toda obligación (sujeto, objeto y relación jurídica) se suman, en este caso, los aspectos particulares del acuerdo celebrado a través de la **vía electrónica** y, en concreto, aquellos referentes a la identidad y representación de las partes, los requisitos de firma y documento escrito a efectos de prueba, así como el de la confidencialidad de las comunicaciones.

Entre los problemas a los que se enfrentan las comunicaciones a través de Internet se encuentra el relativo a la autoría de las mismas, de suerte que es preciso crear mecanismos que permitan verificar la identidad de las partes (emisor y receptor), máxime si se considera que son ellos quienes participan en la creación de los deberes y obligaciones.

El problema fundamental que plantean las transacciones a través de Internet y de cualquier otro medio tecnológico, analizado desde una perspectiva jurídica posee cuatro aspectos que son: **la autenticidad, la integridad, la confidencialidad y el no repudio**, la solución de estos cuatro aspectos se torna un elemento esencial cuya presencia determina

la existencia de las obligaciones concertadas a través del uso de *nuevas tecnologías*, y que consecuentemente determinan las condiciones de validez y prueba del acto jurídico.

Estos cuatro aspectos de la problemática jurídica son consecuencia de que el *mensaje de datos* y en general cualquier documento enviado a través de Internet puede ser interceptado o alterado por cuanto el correo electrónico es transmitido por medio de una **red** abierta <sup>(87)</sup> donde los documentos electrónicos viajan a través de innumerables ordenadores interconectados y las probabilidades de que sus contenidos sean interceptados son considerables, y si a ello sumamos el hecho de que el remitente puede ser un impostor, se hace preciso poder verificar la *autenticidad de la autoría de los mensajes de datos*, lo que se lograría a través de proteger los datos personales de toda persona con la que se tenga algún tipo de relación y que se sometan al cumplimiento de requisitos recurrentes preestablecidos en los sistemas electrónicos o digitales, que garanticen ~~sus~~ la confidencialidad y autenticidad de sus datos, dándole el sentido que la Empresa quiso darle.

### **3.5. Implicaciones de una ley en materia de protección de datos personales en las Empresas.**

Durante los últimos años ha habido un importante desarrollo normativo en materia de protección de datos personales, en una primera instancia, con la entrada en vigor de las leyes de transparencia, las que contemplan apartados específicos en materia de protección de datos personales en el sector público, y posteriormente con las reformas a los artículos 16 y 73 constitucionales en 2009, en los que se otorga reconocimiento pleno a la protección de datos personales como un derecho fundamental y autónomo.

Los repentinos cambios en la forma en que nos comunicamos y en la que vemos al mundo, se ven reflejados necesariamente en la sociedad y por tanto en el campo Empresarial, el Derecho es un fenómeno social y su contenido, depende necesariamente de la forma en que la sociedad se transforma, lo que trae aparejado el surgimiento de nuevas situaciones jurídicas que nunca imaginamos fueran posibles tales como: el **tratamiento legítimo**, controlado e **informado**, a efecto de garantizar la **privacidad y el derecho a la autodeterminación informativa de las personas**, obligando al sector Empresarial a velar,

---

<sup>(87)</sup> Una distinción es importante a efectos de todo el posterior análisis jurídico. Es necesario tener presente que la información "multimedial" compuesta por imágenes, sonidos y datos puede transmitirse mediante redes cerradas o privadas y abiertas o públicas.

Las primeras posibilitan un mayor grado de seguridad, son de propiedad y administradas por entes específicos, y no admiten el ingreso de terceros no autorizados o no habilitados. Mientras que las segundas, como el Internet, no poseen un punto de control central, pudiendo tener acceso cualquier persona en cualquier parte del mundo.

responder, así como rendir cuentas al titular sobre el tratamiento de sus datos personales, valiéndose de estándares y mejores prácticas, así como de esquemas de autorregulación.

Entre los diversos instrumentos internacionales que en materia de protección de datos sustentan las acciones tomadas por el gobierno mexicano destacan:

- La Organización para la Cooperación y el Desarrollo Económicos (OCDE).
- La Organización de las Naciones Unidas (ONU).
- El Foro de Cooperación Económica de Asia Pacífico (APEC).
- El Tratado de Libre Comercio con la Unión Europea.
- La Alianza para la Seguridad y la Prosperidad de América del Norte.
- La Red Iberoamericana de Protección de Datos.
- El Comité Trilateral para el Flujo Transfronterizo de Información.

La cuestión estriba entonces en determinar cuál es el contenido esencial de los derechos; los principios y características que lo definen y que no pueden ser desconocidos so pena de desconocer y en consecuencia violentar el propio derecho. Principios todos ellos recogidos en la LFPDPPP (artículo 6 de la Ley y artículos 9 ss. Reglamento); que para que éstos sean efectivos requieren el reconocimiento garantía y tutela de los derechos de acceso, rectificación, cancelación y oposición (regulados en los artículos 87 y ss. Del Reglamento).

**Los principios internacionalmente reconocidos**, la Directiva 95/46/CE recoge los principios de finalidad, calidad del dato, información, consentimiento y seguridad.

Por su parte, el marco de privacidad de Asia Pacífico (APEC), incluye también los principios que deben regir el tratamiento de datos por las economías miembro, de modo que reconoce los siguientes: Prevención del daño; aviso; limitación de recolección; usos de la información personal; elección; integridad de la información personal; medidas de seguridad; acceso y corrección.

A continuación se muestra una tabla que compara los principios internacionalmente reconocidos: <sup>(88)</sup>.

---

<sup>(88)</sup> ORNELAS NÚÑEZ, L., Curso Ley Federal de Protección de Datos Personales en Posesión de los Particulares y sus Reglamento, Tirant Lo Blanch Formación. México, 2012

Principio/Deber	LFPDPPP	Directrices de la OCDE	Convenio No.108	Directiva 95/46/CE	Resolución de Madrid	Marco de Privacidad APEC
Licitud	✓	✓	✓	✓	✓	✓
Consentimiento	✓	✓	❖	✓	✓	✓
Información	✓	✓	✓	✓	✓	✓
Calidad	✓	✓	✓	✓	✓	✓
Finalidad	✓	✓	✓	✓	✓	✓
Lealtad	✓	✓	✓	✓	✓	✓
Proporcionalidad	✓	✓	✓	✓	✓	✓
Responsabilidad	✓	✓	❖	❖	✓	✓
Seguridad	✓	✓	✓	✓	✓	✓
Confidencialidad	✓	❖	❖	✓	✓	❖

(F9) Tabla que compara los principios internacionalmente reconocidos.

Derivado de lo anterior, como garantía del derecho fundamental a la protección de datos personales, el legislador mexicano ha visto, en los artículos 6 de la LFPDPPP y 9 del Reglamento, que todo tratamiento de datos esté sujeto a los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

Además de los principios, la normatividad prevé los deberes de seguridad y confidencialidad, a los que presta atención el legislador ante la experiencia internacional que se concreta en la consagración de dichos principio en diferentes formas e instrumentos jurídicos internacionales <sup>(89)</sup> que van desde las Recomendaciones de la Organización para la Cooperación y el Desarrollo Económico hasta la resolución de Madrid <sup>(90)</sup>.

Ahora bien, en el ámbito Internacional, cabe destacar la labor de la Organización para la Cooperación y el Desarrollo Económico (OCDE), organismo multilateral que ha elaborado importantes lineamientos y políticas sobre privacidad y protección de datos y protección al consumidor en el contexto del comercio electrónico, entre los más importantes. Aún y cuando las guías o lineamientos que emite la OCDE no son obligatorias para muchos países

(F9) Diseño Diana Márquez Cisneros

(89) En relación con los principales instrumentos internacionales en materia de protección de datos personales que han sido tenidos en consideración para la elaboración de la LFPDPPP, véase Ornelas Núñez, L. y López Ayllón, S., "La recepción del Derecho a la protección de datos en México: Breve descripción de su origen y estatus legislativo", en Protección de datos personales: Compendio de lecturas y legislación, Instituto Federal de Acceso a la Información Pública, México 2010. pp. 57 a 75.

(90) Estándares Internacionales sobre Protección de Datos Personales y Privacidad (Resolución de Madrid), adoptada durante la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada el 5 de noviembre de 2009 en Madrid. La Resolución de Madrid está disponible, en español, en la siguiente dirección de Internet. [http://www.agpd.es/portaIwebAGPD/canaIdocumentacion/conferencias/common/pdfs/31\\_conferencia\\_internacional/estandar\\_es\\_resolucion\\_madrid\\_es.pdf](http://www.agpd.es/portaIwebAGPD/canaIdocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandar_es_resolucion_madrid_es.pdf)

en el ámbito del derecho internacional público, estos son principios generalmente aceptados como recomendaciones de carácter voluntario comúnmente adoptadas por gobiernos, Empresas, organizaciones y usuarios individuales de países miembros de la OCDE, como es el caso de México.

Las Guías de la OCDE que regulan la Protección de la Privacidad y los Flujos Transfronterizos de Datos Personales del 23 de Septiembre de 1980 (8) contienen ocho principios complementarios de aplicación nacional y cuatro principios de aplicación internacional que son considerados como los estándares mínimos a seguir para la obtención, el procesamiento de datos y el libre flujo transfronterizo de datos para los sectores público y privado.

Los ocho principios de aplicación a nivel nacional son los siguientes:

1. El principio de Límite de Obtención, consistente en la imposición de límites para la obtención de datos personales mediante medios apropiados y legales haciéndolo del conocimiento y obteniendo el consentimiento;
2. El principio de Calidad de los Datos, consistente en la importancia de asegurar la exactitud, totalidad y actualización de los datos;
3. El principio del Propósito de Descripción, consistente en especificar el propósito de recabar información en el momento en el que se lleva a cabo la recolección y el subsecuente uso limitado del cumplimiento de dicho propósitos u otros que no sean incompatibles con aquellos propósitos especificados en cada ocasión;
4. El principio del Límite de Uso, consistente en no divulgar los datos personales o aquellos utilizados para propósitos distintos a los contemplados en el principio anterior, excepto:
  - a) el consentimiento sobre la materia de datos;
  - b) mediante una autoridad contemplada en ley.
5. El principio de Protección a la Seguridad, consistente en proteger los datos personales e información, mediante mecanismos razonables de seguridad en contra de riesgos tales como pérdida, acceso no autorizado, destrucción, utilización, modificación o divulgación de datos;

6. El principio de Imparcialidad, consistente en establecer políticas generales de imparcialidad sobre desarrollos, prácticas y políticas con respecto a los datos personales, asegurando la transparencia en el proceso de obtención de información y estableciendo los propósitos para su utilización;
7. El principio de Participación Individual, consistente en el derecho que tiene un individuo de: obtener del controlador de datos la confirmación de tener o no los datos del individuo; que el controlador de datos se lo haya comunicado en un tiempo y forma razonable; obtener respuesta del controlador de datos si una solicitud le ha sido negada y tener la posibilidad de impugnarla; tener la posibilidad de impugnar datos personales y si la impugnación resulta exitosa solicitar que los datos sean eliminados, modificados, rectificados o complementados; y
8. El principio de Responsabilidad, consistente en la responsabilidad del controlador de datos de cumplir efectivamente con medidas suficientes para implementar los siete principios anteriores.

Es importante mencionar que el derecho a la autodeterminación informativa se refiere al poder de disposición y control y faculta a un individuo para decidir cuáles de sus datos proporciona a otros <sup>(91)</sup>.

En la legislación mexicana, como en el caso de la Directiva 95/46/CE, “*el responsable del tratamiento*” es un concepto que tiene un significado autónomo. El modelo europeo, la LFPDPPP define al responsable del tratamiento de datos personales como la “*persona física o moral de carácter privado que decide sobre el tratamiento*” (Artículo 3, fracción XIV).

Con base en esta definición, es posible identificar al menos, dos requisitos para actuar con el carácter de **responsable**. A saber: i) ser una persona física o moral de carácter privado y ii) tener el poder de decisión sobre el tratamiento de los datos personales.

Los elementos para ser considerado responsable del tratamiento, es con motivo de las actividades concretas que realicen las personas, sean físicas o morales de carácter privado, que se podrá identificar a un responsable del tratamiento en la vida práctica.

---

<sup>(91)</sup> Véase el Dictamen de las Comisiones Unidas de Gobernación y de Estudios Legislativos, a la Minuta con Proyecto de Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Este Dictamen tiene fecha del 27 de abril de 2010 y está disponible en la página de la Suprema Corte de Justicia de la Nación, en la liga <http://www2.scjn.gob.mx/red/leyes/>, al acceder al apartado “Procesos Legislativos” de la LFPDPPP.

Los principios para el tratamiento de los datos personales están previstos en los artículos 6 de la LFPDPPP y 9 de su Reglamento, y son los siguientes:

1. Consentimiento
2. Información
3. Finalidad
4. Calidad
5. Proporcionalidad
6. Licitud
7. Lealtad
8. Responsabilidad

Por el otro lado, la figura del encargado está prevista en el artículo 3 de la LFPDPPP, fracción IX, y es definida como la *“persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable”*.

En ese orden de ideas, el artículo 49 del Reglamento de la LFPDPPP especifica, sobre la figura del encargado, que es ajeno a la organización del responsable y que los datos que trata por cuenta de éste, lo hace como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación.

La relación entre el responsable y el encargado del tratamiento, de acuerdo con el artículo 51 del Reglamento de la LFPDPPP, debe quedar establecida mediante cláusulas contractuales o cualquier otro tipo de instrumento jurídico, a efecto de que se pueda acreditar la existencia de la relación y se precise su alcance y contenido, dentro de sus principales obligaciones es abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente.

El problema, en términos prácticos, es que al encargado no le es concedido un tiempo, por disposición legal, para adjuntar o deslindar posibles responsabilidades en el tratamiento de datos personales en su relación con el responsable. Misma situación para efectos de prueba. Esta omisión en señalar un periodo de bloqueo para los encargados, podría influir negativamente en caso de que tuvieran la necesidad de demostrar su cumplimiento.

Por el contrario, la definición de *“tercero”* conforme al artículo 3 de la LFPDPPP señala que es la *“persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos”*. En México, las reglas básicas para que una transferencia de

datos se realice adecuadamente consisten en que el titular haya consentido o dado su permiso para que sus datos sean proporcionados a un tercero <sup>(92)</sup> lo cual debe ser captado por el responsable al hacer del conocimiento del titular esta circunstancia en el aviso de privacidad; y que la transferencia se limite a la finalidad que la justifique, la cual también tiene que ser enterada al titular.

Esto es, el responsable que tenga la intención de transferir datos personales tiene también que comunicar al tercero o terceros el aviso de privacidad, a efecto de que conozcan cuáles fueron los términos pactados con el titular para la utilización de su información.

Del mismo modo, cuando el tercero o “nuevo responsable” obtenga los datos por medio de una transferencia consentida, tiene que hacer del conocimiento del titular el aviso de privacidad. Sin embargo, si este tercero pretende utilizar los datos para una finalidad distinta de la consentida por el titular, entonces debe enterar de esta circunstancia a su titular por medio del mismo aviso, antes del aprovechamiento de la información <sup>(93)</sup>.

En la actualidad, pocas actividades comerciales se escapan de la utilización de datos personales para completar sus ciclos; bien sea que el uso de los mismos constituya una tarea principal o accesoria en el contexto de las operaciones de la organización, que su tratamiento se haga en sistemas físicos o automatizados, o que incluso se pueda llevar a cabo en línea.

Derivado de lo anterior, es clave que todas las Empresas que participan en cualquier relación jurídica que involucre el manejo de información personal tengan claro su papel, en tanto que así sabrán cuáles son sus deberes al respecto. También, es importante mencionar que el buen manejo de la información de cada persona puede ayudar en la prevención de fraudes de identidad.

En el mundo, los fraudes de identidad son algo cotidiano. Se estima que cada cuatro segundos ocurre un robo de identidad, y su resolución requiere un promedio de 600 horas de trabajos de investigación. Es responsabilidad de cada Empresa crear y vivir una cultura

---

<sup>(92)</sup> Al respecto, el numeral IX del Marco de Privacidad de APEC, denominado “Responsabilidad”, señala que cuando la información personal vaya a ser transferida a otra persona u organización, nacional o internacional, el controlador de la información personal (responsable) debe obtener consentimiento del individuo (titular) o actuar con la debida diligencia y tomar las medidas razonables para asegurar que la persona u organización receptora, protegerá la información consistentemente con los principios de dicho Marco.

<sup>(93)</sup> Véase el artículo 29 del Reglamento de la LFPDPPP.

de protección de datos personales, sensibilizando a quienes están en su ámbito de influencia (empleados, colaboradores, clientes y proveedores) para evitar sanciones.

Aquí es donde hace su aparición el Derecho ante este tipo de situaciones, el cual a mi juicio en el marco de la llamada “*sociedad del conocimiento*”, los profesionales del Derecho Empresarial debemos estar preparados para dar solución a los problemas jurídicos de las organizaciones derivados del tratamiento legítimo, incorporando al estudio de la dogmática jurídica la cultura de protección de los Datos Personales que fortalezcan el esquema legal para dar certeza a las transacciones comerciales; toda vez que en la actualidad la estructura de las Empresas, la cantidad de datos personales que manejan y la cultura de estas organizaciones hacen que **no puedan adaptarse de manera ágil** a la regulación que entró en vigor hace cinco años.

Por el contrario, la citada ley ha generado sanciones a las Empresas, ante su falta de cumplimiento, pero la mayoría de las multas son **por no saber proteger los derechos de los usuarios o clientes**. A continuación señalamos algunos aspectos importantes en materia de privacidad que desconocen las organizaciones:

- **Manejo de los datos**
- **Sujetos que intervienen en la relación jurídica**
- **Nuevas obligaciones**
- **De los derechos de Acceso, Rectificación, Cancelación y Oposición**
- **La transferencia nacional e internacional**
- **Procesos de verificación**
- **Nuevas multas**
- **Sanciones penales**
- **La autoridad garante**
- **Publicidad negativa**
- **Acciones por daño moral**
- **Pérdida de la confianza de clientes y empleados**
- **Códigos de ética y autorregulación de la industria**

De acuerdo a los requerimientos de la LFPDPPP se propone el siguiente modelo para definir e implementar una estrategia para la protección de datos personales en posesión de particulares, con el objetivo de proporcionar dirección y soporte para el cumplimiento de dicha ley.



(F10) Modelo para la implementación de una estrategia para el cumplimiento de la LFPDPPP.

El campo de la informática jurídica, considera el aspecto instrumental de la informática al servicio del Derecho, o al menos así es como lo considera PIÑA-LIBIEN <sup>(94)</sup> y algunos otros juristas, para quienes dentro de su objeto de estudio y contenido, el Derecho Informático debe incluir lo siguiente:

- A. **Protección de la privacidad:** Derecho fundamental, tener acceso a los datos personales y a corregir datos erróneos, sin coartar la libertad de recolección de la información.
- B. **Libertad de información:** Es indispensable adoptar un criterio sobre este término, para permitir un mayor acceso a los datos que poseen las Empresas, instituciones y el gobierno, sin perjuicio de éstas.
- C. **Criminalidad y fraude informático:** Este tema es muy complejo, ya que según el Derecho Penal se denomina robo: “el apoderarse con fuerza o violencia de bienes ajenos” y fraude informático al acceso indebido a la información, muchas veces no para apoderarse de ella, sino con la intención de modificar datos.

(F10) Diseño Diana Márquez Cisneros

(94) PIÑA-LIBIEN, Hiram Raúl, **Proyecto: Base Bibliográfica de Derecho Informático**, [En línea] Comunidad Alfa-REDI. <http://www.alfa-redi.org/base/base-sp.asp> [Consulta: 15. mar. 15]. Para este autor como coordinador del proyecto, si se toma a la informática en todos sus aspectos, como objeto del Derecho, ello implica considerar entonces al Derecho Informático.

- D. **Problemas de soberanía:** Relativo al flujo de datos transfrontera, en la medida que ésta pueda poner en peligro la soberanía nacional. Es un problema muy grave en países en vías de desarrollo, ya que su dependencia tecnológica lo pone en una situación crítica.
- E. **Otras prioridades:** Se refiere a las reformas jurídicas que necesariamente han de efectuarse en materias de derechos de autor, seguros, contratos y modificaciones de las leyes, puesto que la mayoría de los problemas informáticos con la justicia derivan de la dificultad de adaptar las leyes vigentes a las nuevas tecnologías.

En cuanto a lo que denomina protección a la privacidad <sup>(95)</sup>, se habla acerca de las pautas que deben fijarse para la recolección de los datos, estableciendo en términos más o menos exactos, cuales son de carácter público y cuales son considerados privados, además de que considera que debe establecerse y garantizarse el derecho de toda persona a utilizar y servirse de la tecnología, que solo se limitará cuando los datos sean de carácter personal, lo que estará sujeto a las disposiciones de la ley.

Sin embargo, el uso claro y preciso de la información define el objeto como ya se señaló anteriormente, del derecho a la protección de datos y utilización de la información, que garantice la seguridad de la información y tomar las medias técnicas para impedir el acceso no autorizado a los sistemas y la adopción de las medidas jurídicas para castigar legalmente a los responsables cuando esto llegase a suceder, definiendo las responsabilidades de los administradores de la información, por el manejo indebido de los datos.

El problema real radica no solo en la delimitación del objeto de estudio de la Protección de Datos Personales, sino que se hace polémica desde la denominación de la materia y hasta el objeto de estudio de la misma ante la falta de cultura en las Empresas al respecto que permitan el aprovechamiento del conocimiento.

### **3.6. La protección de datos en el ámbito de la mercadotecnia.**

La importancia de la información y los grandes volúmenes de datos que se manejan en el mundo, las revoluciones tecnológicas y digitales, la información sensible de las personas se han convertido en moneda de cambio para **el marketing** y para muchas

---

<sup>(95)</sup> *Íbidem.*

Empresas que no tienen claro lo que es salvaguardar y proteger los datos que albergan en sus bases de información.

Mientras muchas Empresas siguen haciendo uso indebido de la información que las personas les han confiado, los call center, las agencias de viajes, Empresas dedicadas a llamar al cliente para ofrecer las grandes promociones y diversas instituciones bancarias (por mencionar sólo algunos ejemplos) no cesan en el bombardeo telefónico, postal y digital; provocando no sólo descontento sino vulnerabilidad en grandes sectores de la población. Y es que el marketing, tradicionalmente ha buscado las herramientas para atraer a nuevos clientes, así como para fidelizar a los que ya lo son, o para posicionar en las mentes de los consumidores una marca o un producto para que sea su principal opción al momento de cubrir sus necesidades.

La promoción, es una de las herramientas principales del marketing o de la comunicación de las Empresas para cumplir sus metas y dentro de la promoción se encuentran acciones concretas como la publicidad, las promociones de ventas, las relaciones públicas o la venta directa a consumidores. Es en este último punto donde la progresiva implantación en el tráfico mercantil y Empresarial de las tecnologías de la información, ha transformado las herramientas del marketing tradicional y donde han nacido instrumentos como el marketing directo donde las organizaciones Empresariales pretenden obtener respuestas medibles a sus campañas, en un público objetivo (target) determinado. En ese orden de ideas, mencionaré los riesgos legales de utilizar las formas tradicionales de marketing directo como el mailing postal tradicional, el telemarketing o las más recientes formas como el envío de emails (marketing online) o SMS o MMS publicitarios. Más allá de la forma o el canal escogido para comunicarse con los potenciales consumidores, ha cambiado también el mensaje que se les envía aumentando, de forma muy considerable, la capacidad de interacción entre la Empresa y el consumidor o, incluso, entre los propios consumidores (un buen ejemplo de esto serían las campañas lanzadas cada vez con mayor frecuencia a través de redes sociales).

Uno de los principales objetivos de las campañas de marketing actuales, es conocer al consumidor; si se llega a un punto de conocimiento óptimo del destinatario de su mensaje, las posibilidades que este reaccione positivamente al mensaje lanzado, aumentan considerablemente. Volviendo nuevamente a los expertos en materia de marketing, estos enumeran en tres, los ingredientes para que una campaña de marketing directo tenga opciones de ser exitosa: el primero disponer de una base de datos; el segundo la

interactividad y la participación del destinatario del mensaje y en tercer lugar conseguir motivar su participación (respuesta positiva). El nivel de perfeccionamiento, sin embargo no acaba aquí, ya que también se habla del database marketing (marketing de base de datos), que se diferencia del marketing directo en un mayor análisis de los datos disponibles de los consumidores (bien sean personas físicas o jurídicas), procediendo a su filtrado para conocer aún más al destinatario del mensaje (creación y análisis de perfiles), resultando el mayor o menor éxito de sus acciones, en función de la cantidad de información de que puedan disponer de un consumidor determinado. El marketing apunta pues hacia el conocimiento del consumidor con el objetivo de personalizar el mensaje que recibe.

Sin embargo el presente trabajo está dirigido al sector Empresarial quién, sin disponer de sofisticadas herramientas informáticas para analizar los datos del negocio y de qué dispone, tienen la necesidad de promocionar sus productos o servicios a nuevos clientes o mercados. No se debe olvidar que el marketing o la estimulación de la demanda, forma parte de los objetivos básicos de cualquier organización Empresarial. Para tratar de dar una visión global, no me centraré, únicamente en las nuevas formas de comunicación con clientes (cómo el email o el SMS o MMS), sino que mencionaré cualquier canal de difusión de la oferta existente en este momento, siempre que el mensaje sea enviado a una persona (física o jurídica) determinada, con el objetivo final que prácticamente cualquier Empresa que promocione sus productos o servicios de esta forma, pueda evitar sanciones que tengan impacto en sus resultados financieros.

A través de esta breve definición de la evolución de las herramientas de promoción dentro del marketing y de las tendencias actuales, enumeraré algunos de los elementos jurídicos relevantes integrantes del envío de un mensaje publicitario personalizado, que trataré en el presente trabajo:

1. El envío de un mensaje de este tipo, con independencia del canal de comunicación utilizado, presupone que su remitente (normalmente, aunque no necesariamente, la Empresa que quiere promocionar sus productos o servicios), dispone de un cierto grado de información, mayor o menor, del destinatario, al menos de algún dato que permita enviarle información comercial por cualquier medio: dirección postal, dirección electrónica, número de teléfono fijo o móvil, etcétera.
2. Esta información, puede consistir en datos de carácter personal o no.

3. Los datos de que dispone el remitente pueden ser de clientes o de personas, físicas o jurídicas, que nunca hayan adquirido sus productos o servicios.
4. Esta información puede tener diferentes orígenes: la base de datos de clientes o clientes potenciales propios, la base de datos de otras Empresas del sector o que comercializan bases de datos, otra Empresa del mismo grupo, etcétera.
5. El envío de la comunicación comercial, supone una forma de tratamiento de los datos de su destinatario.

Conocer si la información de la que dispone quien realiza la acción de marketing, es considerada un dato personal o no, no es una cuestión insignificante, pues resulta clave para conocer si ese tratamiento de datos concretos está o no sujeto a la LFPDPPP, en consecuencia, si nos encontramos o no ante un derecho, de los considerados, fundamentales por la Constitución Española.

La LFPDPPP define como dato personal como “cualquier información concerniente a una persona física identificada o identificable”. Por tanto de la definición legal de dato personal podemos concluir, que tendrá esta consideración la información relativa a una persona física, que permita identificarla de forma directa o que sea identificable a través de la citada información.

Las características para conocer cuando una información puede o no ser considerada como dato personal en muchas Empresas que implantan la normativa de protección de datos en su organización. Este problema jurídico se plantea debido a que la normativa de protección de datos no regula únicamente los datos íntimos, como he señalado más arriba, sino cualquier dato personal, íntimo o no, y no cabe duda que la información relativa a profesionales y comerciales individuales, con independencia de la actividad llevada a cabo por estos, cumple con la definición de dato personal “persona física identificada o identificable”.

Así pues, las agencias de publicidad a las que se les encarga la creación y desarrollo de las campañas de comunicación para sus clientes, en donde la creatividad del concepto, diseño y desarrollo, es la pieza clave del éxito de las mismas, teniendo siempre en cuenta los objetivos comerciales deseados (ventas y posicionamiento de la marca), así como el

público objetivo o target (grupo de personas o sector de la sociedad para quienes está destinado el nuevo producto o servicio). Mencionaré la clasificación por actividad:

- I. Agencias de publicidad
- II. Empresas de investigación de mercado
- III. Empresas de mercadotecnia directa
- IV. Empresas recolectoras y comercializadoras de bases de datos
- V. Centros de contacto (call centers)
- VI. Empresas de tarjetas de crédito
- VII. Bancos
- VIII. Buros de crédito
- IX. Tiendas departamentales
- X. Empresas en general

### **3.7. Las 5 claves para cumplir con la Ley Federal de Protección de Datos Personales por parte de las Empresas.**

El presente trabajo pretende ser un instrumento más para clarificar los alcances de las Empresas y servir de apoyo para que ajusten sus actividades cotidianas en el tratamiento o manejo de datos personales con lo que dispone la normatividad aplicable a la materia. Ante el escenario de la LFPDPPP, las Empresas tienen una mayor responsabilidad de resguardar la información de sus clientes, pero más allá de este requerimiento legal, se abre una oportunidad de negocio para capitalizar el valor de contar con datos maestros, seguros y confiables para utilizarlos de manera correcta en su toma de decisiones.

En el marco legal, que refiere directamente a la garantía del cumplimiento con la Ley Federal de la Protección de Datos, se solucionaría mediante un tercero que mejorará el seguimiento, la transparencia y la capacidad de auditoría de datos personales y financieros. La confianza para tomar decisiones en toda una Empresa se dará de forma orgánica gracias al incremento de precisión, fiabilidad y puntualidad de los datos críticos para el negocio.

Otro punto a destacar es el papel que juega el enmascaramiento de datos, software que proporciona funcionalidades en tiempo real para evitar que los usuarios no autorizados tengan acceso a información confidencial. Es importante aplicar reglas de enmascaramiento de datos sofisticados y flexibles basados en el nivel de autenticidad del usuario, para ocultar dinámicamente la información sensible, así como bloquear, auditar y alertar a los usuarios finales, al personal de tecnologías de la información y a los equipos externos que tienen acceso a los datos confidenciales. De esta forma, se garantiza un cumplimiento rápido de las normativas en materia de privacidad. Además, al ocultar la información se reduce el riesgo

de una filtración de datos, con la facilidad de adaptar la solución a una normativa o requisitos de negocio específicos.

Por otra parte, se resguardan los datos confidenciales (tarjetas de crédito, direcciones postales y números telefónicos) frente a una exposición accidental mediante la creación de datos realistas y disociados que se puedan compartir de forma segura tanto con usuarios internos como externos, por ejemplo, cuando le llega vía correo su estado de cuenta bancaria se usa una solución de ocultación de datos, lo que asegura el cumplimiento de las normativas y disposiciones relacionadas con la privacidad de la información.

En nuestro país, las Empresas no acatan la ley, por lo que en el presente trabajo recomiendo seguir las reglas siguientes:

- **Crear una carpeta de cumplimiento y el Departamento de Protección de Datos.**
- **Capacitación al interior de la organización.**
- **Crear el aviso de Privacidad.**
- **Derechos ARCO.**
- **Medidas de seguridad.**

Contamos con 4 años y medio de que entró en vigor la LFPDPPP en México y está comenzando a evolucionar **de un tema consultivo o cuestiones litigiosas**, en las que cada vez con más frecuencia, coloca a las Empresas en situaciones difíciles en caso de no tomar medidas para cumplir con la Ley. Las organizaciones deben crear una estrategia enfocada que proteja la información más importante y que responda rápidamente cuando ocurra una violación.

En la 13a Encuesta Global de Seguridad de la información (EGSI) y comparativo México, se analizaron los pasos que las Empresas están dando para abordar los riesgos nuevos o que van en aumento. Según los encuestados, los tres controles principales que las organizaciones están implementando son: ajustes a políticas (39%), más actividades de concientización de la seguridad (38%) y técnicas de encriptación (29%).<sup>(96)</sup>

---

<sup>(96)</sup> Fuente: *13a Encuesta Global de Seguridad de la información (EGSI) y comparativo México. Perspectivas sobre los riesgos de TI*, [En línea]: [http://www.ey.com/Publication/vwLUAssets/Seguridad\\_de\\_la\\_informacion\\_en\\_un\\_mundo\\_sin\\_fronteras/\\$FILE/Seguridad\\_de\\_la\\_informacion\\_en\\_un\\_mundo\\_sin\\_fronteras.pdf](http://www.ey.com/Publication/vwLUAssets/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras/$FILE/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras.pdf) [Consulta: 20. abril. 2015].

### **3.7.1. Crear una carpeta de cumplimiento y el Departamento de Protección de Datos Personales.**

Si bien la LFPDPPP habla de una protección a los datos personales, lo que en realidad se protege es el dueño o Titular (persona física) propietaria de éstos datos personales. Por éste motivo, en la mayor parte de los casos, le Ley protege al Titular de éstos datos, por lo que el Responsable está obligado a acreditar el cumplimiento que da a sus obligaciones.

La forma de acreditar éste cumplimiento, es por medio de documentos que contengan en forma clara, las acciones que ha tomado el Responsable para cumplir con los diferentes aspectos de la Ley. Ésta carpeta deberá contener desde las listas de asistencia a las capacitaciones, las entrevistas a las diferentes áreas para obtener la información sobre los diferentes datos, sistemas de tratamiento y transferencias, los avisos de privacidad, políticas en materia de protección de datos personales, contratos de envío o transferencia de datos.

La creación del Departamento de Protección de Datos Personales y en general todas aquellas actividades tendientes a cumplir con la Ley, que sea responsable de dar trámite y contestación a las posibles solicitudes de derechos ARCO y también de fomentar la protección de datos personales dentro de la organización. Sin embargo, la realidad es que las Empresas no saben cómo actuar ante una solicitud ARCO pues carecen tanto de una metodología para recibirla, como de la tecnología para procesarla y responderla en los términos que indica la ley (máximo 20 días). De hecho muchas Empresas no cuentan ni con la tecnología, ni con el personal suficiente y sobre todo calificado para dar respuesta al número de demandas ARCO, esto tomando en cuenta que dar respuesta a una solicitud ARCO puede ser más complicado de lo que parece a simple vista, dado que los datos personales del solicitante se encuentran dispersos en varios departamentos de la Empresa.

### **3.7.2. Capacitación al interior de la Organización.**

Uno de los principales objetivos de la Ley, es **permear la política** de privacidad a toda la organización, ya que si bien el Responsable de la información es la Empresa y ésta puede ser sancionada en caso de un incumplimiento a la Ley, los autorizados a tener acceso a las bases de datos, pueden cometer un **delito** en caso de vulnerar estas bases de datos o recolectar datos en forma engañosa y obtener un lucro de ello.

Por lo que la segunda de las cinco claves para dar cumplimiento con la Ley, es brindar capacitación al personal, ya sea a través de cursos, presentaciones, etcétera. Así mismo darle seguimiento a la capacitación, a través de la elaboración de cuestionarios, para conocer el nivel de comprensión que ha sido captada por los empleados y enfocarse en lo que no fue comprensible para corregirlo de inmediato.

Es importante resaltar que la capacitación debe realizarse de acuerdo al nivel de importancia del manejo de los datos personales, siendo ésta orientada primeramente al personal que por sus funciones desempeñan dentro de la Empresa y que tenga acceso a los datos personales, para generar la cultura deseada. Así mismo la capacitación será en el mismo grado de complejidad, con base al tipo de personal que reciba dicha capacitación. Es importante señalar que el área Directiva es la primera que debe ser capacitada, debido a que es de suma importancia que conozca las obligaciones a las que está sujeta la Empresa ante la Ley. Es importante resaltar, que uno de los objetivos principales de la Ley fue salvaguardar lo más valioso que tenemos como seres humanos, que es **nuestra Privacidad**, y para cumplir con ello debemos modificar muchas de las conductas que hemos aprendido y que pasan por alto este derecho.

La ley nos dice lo que debemos hacer, el reglamento nos dice bajo que reglas, pero cada uno de nosotros debemos establecer el cómo. Asimismo, como he mencionado más del 80% de las vulneraciones de información en las Empresas se da desde el interior de la organización y no desde el exterior, por lo que resulta particularmente importante llevar a cabo **capacitaciones constantes** en la materia, a efecto de que los empleados sepan las **consecuencias** del mal uso de los datos personales que trabajan, tanto para la Empresa como para ellos mismos.

### **3.7.3. Crear el Aviso de Privacidad.**

Por la forma en que ha sido manejado por parte del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI), el aviso de privacidad resulta ser un instrumento fundamental para el cumplimiento de ésta regulación, debe estar alineado a los elementos señalados por el Art. 26 del reglamento y el 16º de la Ley. El aviso de privacidad debe contar con los datos de identificación de la Empresa como responsable de proteger los datos, los datos personales que se recaban (señalando si se trata de datos sensibles y en su caso recabando el consentimiento expreso), así como las finalidades y los tratamientos a los que serán sometidos los datos personales, las organizaciones con las que se comparten datos

(transferencias), y las vías de contacto para ejercer los derechos ARCO, para notificar cambios en el aviso de privacidad a los titulares y los medios que se utilizaran para garantizar la confidencialidad de los datos.

Es importante mencionar que el aviso de privacidad debiera ser el último eslabón de una serie de actividades de análisis de los datos que se tratan al interior de la Empresa, así como de los diferentes sistemas de tratamiento, entre otras actividades, del cual obtendríamos la información necesaria para elaborar el aviso de privacidad. Éste documento es un contrato, por lo que crear y poner a disposición un aviso de privacidad crea derechos para el Titular y obligaciones para el Responsable de los mismos, obligaciones que se deben tener presentes.

#### **3.7.4. Derechos ARCO.**

Los derechos de acceso, rectificación, cancelación y oposición (ARCO), son los derechos que tiene todo Titular de datos personales, los cuales pueden ser ejercidos en cualquier momento por éste o su representante legal ante el Responsable. El aviso de privacidad debe señalar claramente el procedimiento para el ejercicio de éstos derechos. Estos esquemas deberán incluir mecanismos para medir su eficacia con respecto a la protección de los datos personales, así como prever consecuencias y medidas correctivas eficientes en caso de incumplimiento.

Es importante saber que como Responsable de las bases de datos, la Ley obliga a contar con un procedimiento específico, disponible en todo momento a los Titulares para su ejercicio. Como parte de sus responsabilidades están:

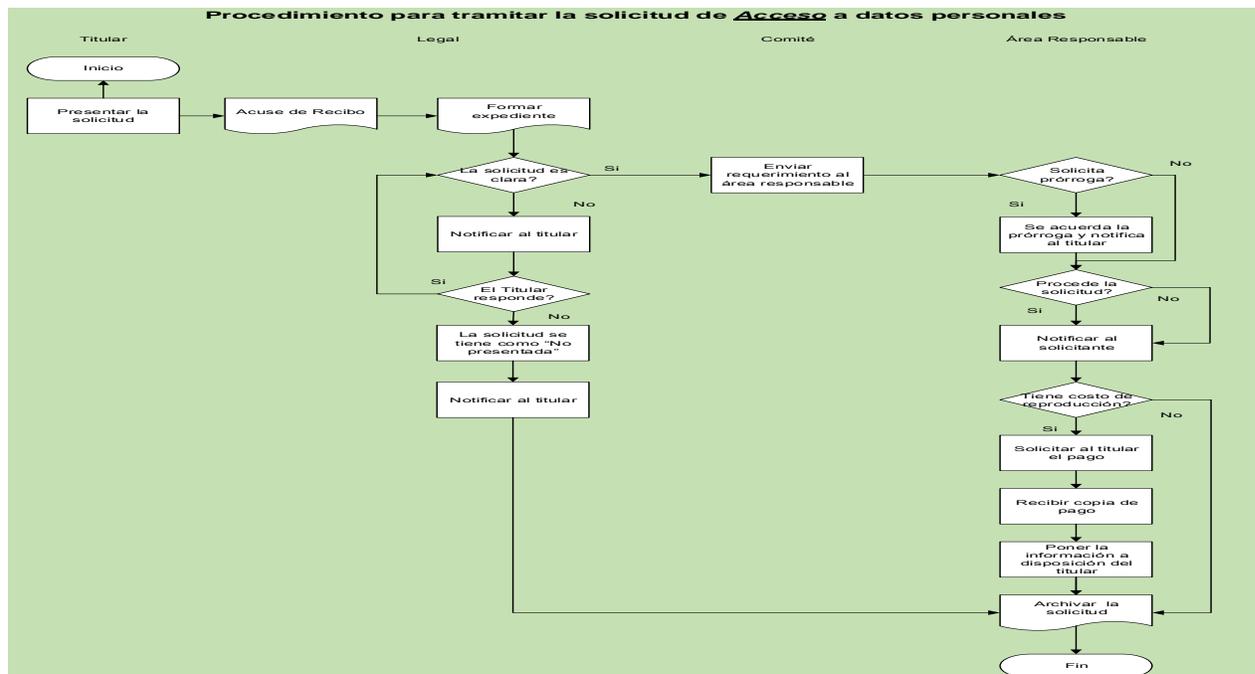
- Tramitar las solicitudes de Derechos ARCO que los Titulares de los Datos Personales presenten a la Compañía.
- Proponer e Implementar al interior de la Organización, todas las políticas y procedimientos necesarios para el adecuado tratamiento de los Datos Personales en posesión de la Empresa.
- Difundir la cultura de la privacidad de Datos Personales en la Empresa.
- Dar asesoría a todas las áreas de la Compañía y a los titulares de los datos personales, respecto a la adecuada protección de los mismos.
- Investigar cualquier posible violación a las Leyes, Principios, Políticas y Procedimientos tendientes a hacer efectiva la Protección de Datos Personales al interior de la Compañía.
- En general vigilar el adecuado cumplimiento de la LFPDPPP al interior de la Organización.

Todo Titular tiene derecho a conocer qué datos personales se recaba y para que los utilizan las Empresas a través de un “Aviso de Privacidad” que es el documento físico, electrónico o en cualquier otro formato (visual o sonoro) generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con lo que establece la Ley. El tratamiento de los datos personales se debe limitar a las finalidades que se informen en el *Aviso de Privacidad*.

- En todo momento, los titulares en relación con sus Datos Personales podrán ejercer sus derechos ARCO.
- Para poder ejercer los derechos ARCO es necesario que el titular envíe una solicitud en formato libre a través de correo electrónico, detallando el derecho que desee ejercer: Acceso, Rectificación, Cancelación, Oposición.
- El tiempo de respuesta para una solicitud es de 15 días hábiles.
- Cuando una solicitud no sea clara, el Comité de Datos Personales debe solicitar al titular solicitante, un correo electrónico requiriendo el detalle de la información.
- Los plazos de conservación de los datos personales no deberán de exceder aquellos que sean necesarios para el cumplimiento de las finalidades que justifican su tratamiento.

En caso de recibir una solicitud de ésta naturaleza, recomiendo seguir los siguientes

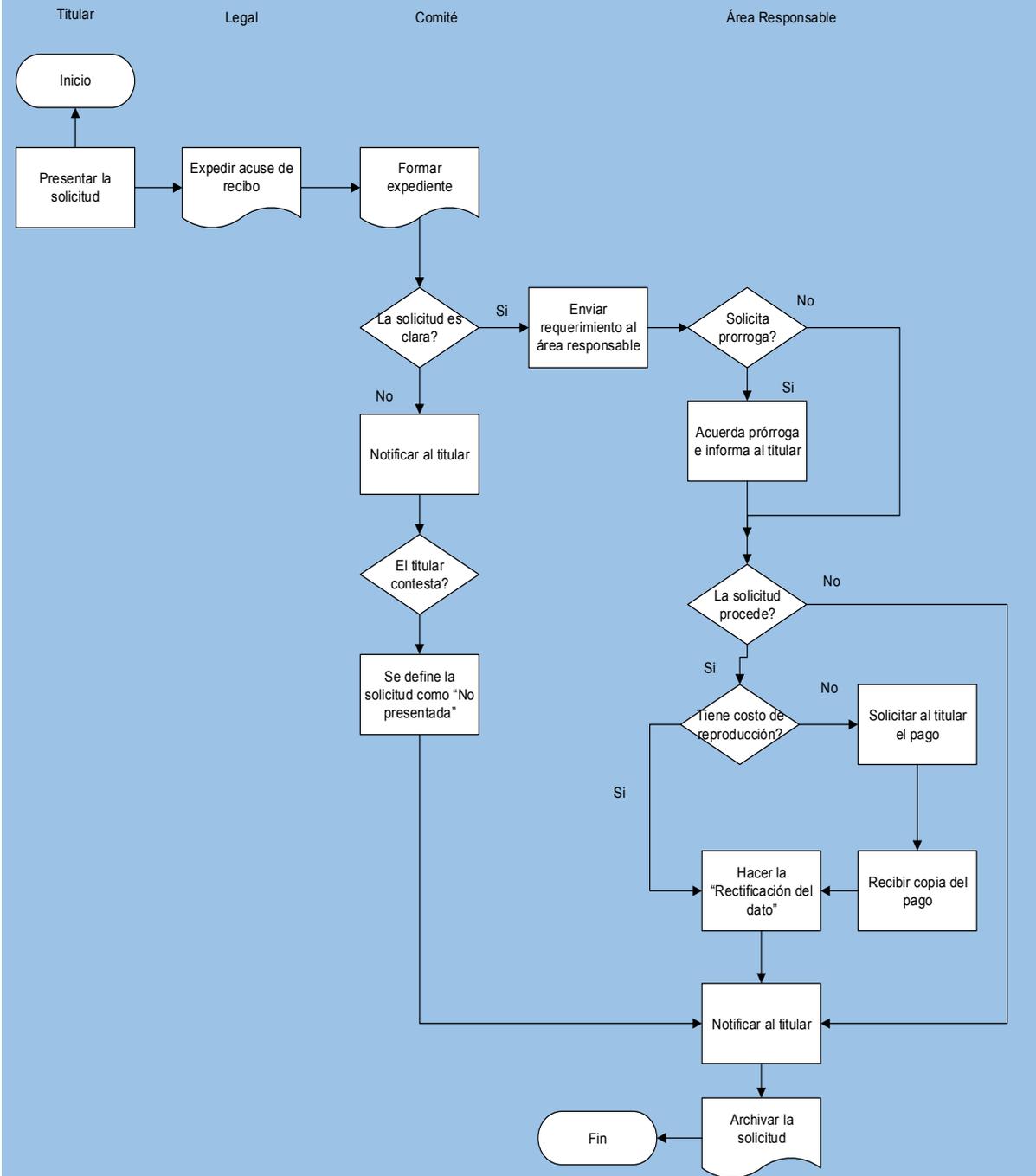
diagramas:



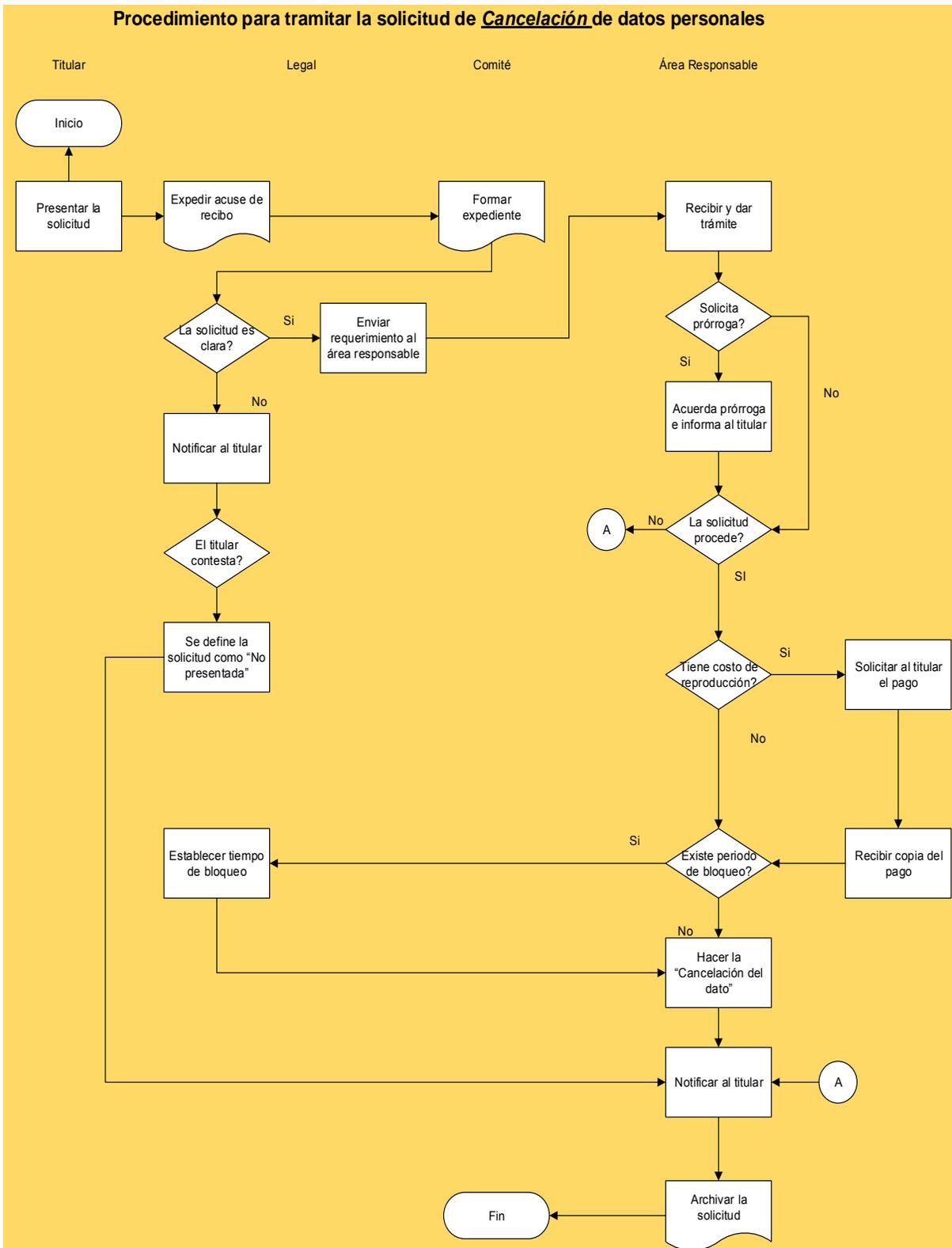
(F11) Gráfico del Procedimiento para tramitar la solicitud de Acceso a datos personales.

(F11) Diseño y contenido original Diana Márquez Cisneros

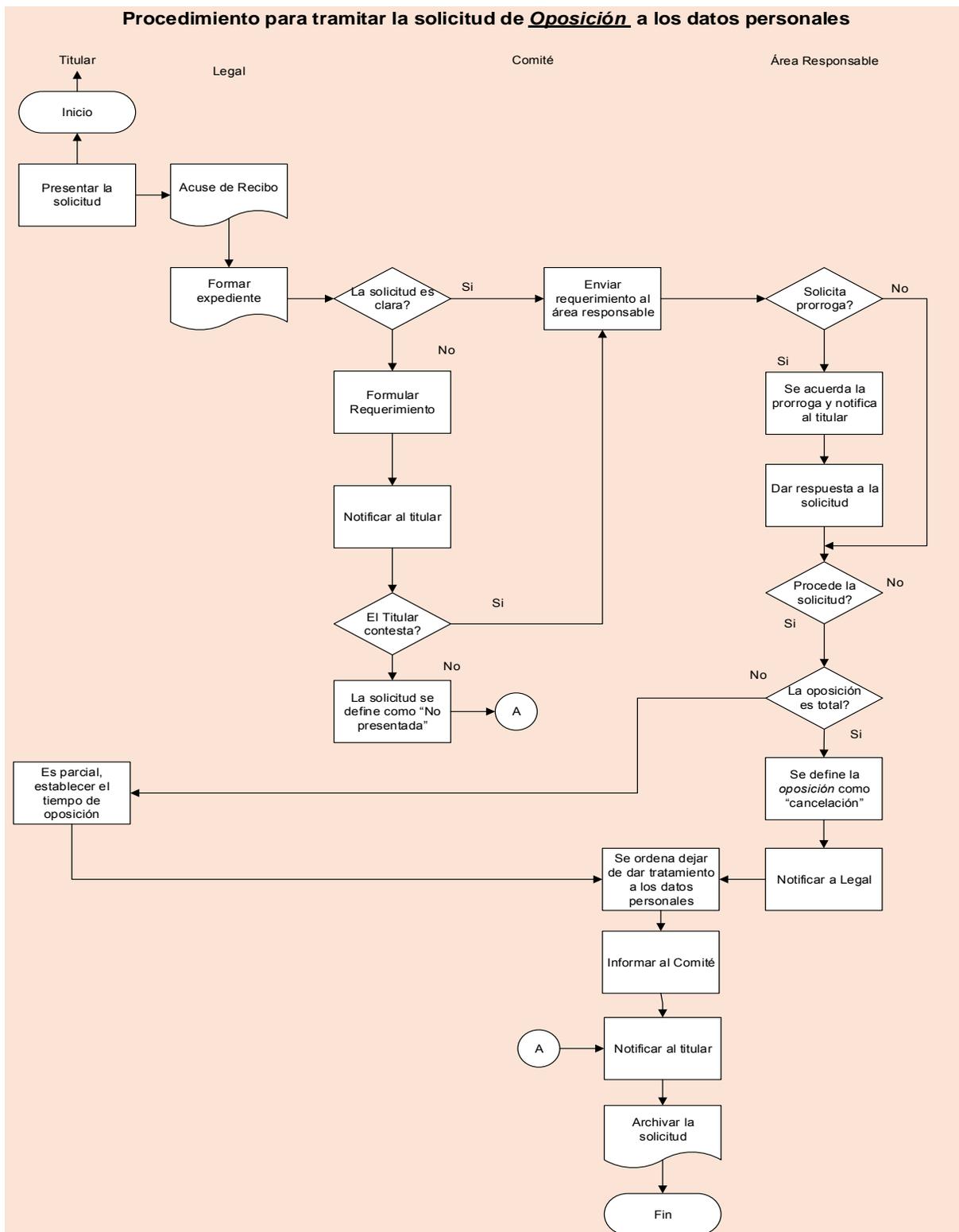
Procedimiento para tramitar la solicitud de Rectificación de datos personales



(F12) Gráfico del Procedimiento para tramitar la solicitud de Rectificación de datos personales.



(F13) Gráfico del Procedimiento para tramitar la solicitud de Cancelación de datos personales.



(F14) Gráfico del Procedimiento para tramitar la solicitud de Oposición a los datos personales.

Uno de los principales aspectos de la LFPDPPP es el reconocimiento de los derechos ARCO, es decir, la facultad que cada persona tiene para exigir a una Empresa u organización el acceso a sus datos personales que de ella tenga así como para solicitar su rectificación, cancelación e incluso oponerse a su uso. El incumplimiento a una solicitud ARCO puede ser sancionado con multas que pueden llegar a alcanzar hasta los trescientos veinte mil días de salario mínimo (18 millones de pesos según la capacidad de la Empresa y las medidas que haya adoptado o no para procurar cumplir con la Ley).

### 3.7.5. Medidas de seguridad.

El reglamento de la Ley contiene un capítulo específico para determinar y documentar las medidas de seguridad físicas, administrativas y técnicas que la Empresa implementa. Estos controles o grupos de controles de seguridad para proteger los datos personales, deben de vincularse con las **recomendaciones** en materia de seguridad de datos personales que ha emitido la autoridad.

Para determinar las medidas de seguridad al interior de la Empresa, se deben **tomar en cuenta factores como:** (i) El riesgo inherente por tipo de dato personal; (ii) La sensibilidad de los datos personales tratados; (iii) El desarrollo tecnológico; (iv) Las posibles consecuencias de una vulneración para los titulares; (v) El número de titulares; (vi) Las vulnerabilidades previas ocurridas en los sistemas de tratamiento; (vii) El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión; y (viii) Demás factores que puedan incidir en el nivel de riesgo o que resulten de otras leyes o regulación aplicable al Responsable.

Al determinar lo anterior, el Responsable **deberá considerar, documentar y actualizar recurrentemente** acciones tales como:



(F15) Gráfico de las acciones del responsable de la base de datos personales.

En ese orden de ideas, cito recomendaciones adicionales sobre las medidas de seguridad mínimas que deben aplicar las Empresas para el tratamiento de los datos:

- Guía de manera general y sencilla sobre los documentos, procedimientos con que deben cumplir por Ley todas las Empresas para la protección de los datos personales.
- Explicar la diferencia entre ceder datos de carácter personal y transferencias.

Aquellos terceros deben reflejar su compromiso con los convenios de Confidencialidad, que sólo nos dice que “no se divulgará información que se conozca en el transcurso del manejo de la información”, pero no garantiza que se pierda, la roben o extraigan. Por ello es necesario validar la seguridad de los terceros a los que se comparten datos de carácter personal, a fin de constatar que cuentan con los mecanismos de seguridad mínimos que establece la Ley, y ver que esto se refleje en un documento donde se comparta la responsabilidad en caso de que los datos personales se pierdan.

Por todo ello es importante perseguir el dato desde su origen, hasta su final destrucción, a través de los procesos del mismo negocio y no en los servidores y aplicativos. Nuestra obligación como profesionales del derecho Empresarial ahora no sólo es para con la infraestructura de las Empresas y sus datos, sino también con nuestros usuarios internos y externos y más aún con nuestros Directivos, a los cuales debemos proteger de las sanciones privativas de libertad y evitar que las utilidades se vayan para el gobierno a través de exorbitantes sanciones, colocando a las Empresas en situaciones difíciles en caso de no tomar medidas para cumplir con la Ley.

### **3.8. El cumplimiento de la LFPDPPP se considera un gasto más que una inversión en las Empresas.**

Las organizaciones no han podido adaptarse a la nueva regulación; es importante subrayar que no sólo datos personales son datos personales sensibles y es ahí donde se añade una complejidad más a todos los procesos que deben llevar a cabo, lo que trae como consecuencia un **cúmulo de sanciones que se deben a la falta de conocimiento** en materia de protección y administración de datos.

Las Empresas en México no necesariamente han estado involucradas en el tema de protección de datos personales y se ha visto como un gasto más que como una inversión, a la fecha éstas organizaciones no han adoptado esquemas de protección de datos

personales que sean capaces de garantizar las bases de datos, incluyendo protocolos internos de actuación y una cultura hacia el respeto y seguridad de la información de los clientes y terceros, que adopten medidas que certifiquen su conservación, previniendo un impacto legal-financiero; diseñando una estrategia de gobierno que sea compartida por toda la organización, que desarrolle políticas orientadas al conocimiento y formación de las nuevas exigencias, con procedimientos sancionadores para el caso de incumplimiento.

El problema es que el sector Empresarial en el ámbito de seguridad considera que es un gasto que se puede evitar, dejando aún lado la legislación y sólo lo consideran cuando les pasa algo. Prepararse para protegerse de un eventual riesgo resulta caro, y por tanto, se posterga. El día en que pasa algo, se asume la conveniencia de estar más protegido. Es como el seguro del auto; si uno no lo tiene, y le pasa algo, viene luego el lamento.

Al Empresario, antes de decirle el costo, hay que convencerlo de que lo que se le está ofreciendo, va a mejorar su productividad, poder demostrarle que con medidas de seguridad, eso podría no haber pasado. Allí quizá se pueda justificar más fácilmente que es una inversión y no un costo. La mayoría de las Empresas poco a poco, van siguiendo la tendencia, entendiendo la importancia de adquirir ciertas conductas de prevención. Claro está, cuando les sucede un contratiempo, eso les lleva rápidamente a tomar medidas. Resulta importante reconocer que hay una falta de preparación frente a los potenciales daños vinculados con la pérdida o mal uso de la información personal, ubicando al riesgo de seguridad respecto de la privacidad, en un máximo histórico en todos los sectores.

Es difícil concientizar a las Empresas ante la necesidad de una inversión importante en seguridad, porque no da un beneficio tangible, salvo que se valore lo que los profesionales evitamos con esas medidas de seguridad. Decirle a un Empresario que instale determinado equipo, que se hagan ciertos procedimientos cada cierto tiempo, son todos costos que se van a sumar; si no pasa nada significa que no se está ahorrando, por el contrario se genera un gasto de dinero por algo que no se sabe si va a pasar.

Las inversiones en infraestructura tecnológica son un gasto oneroso, por lo que cualquier proyecto informático que involucre un cambio de sistema en las Empresas no se asume en la primera revisión, razonablemente, debería ser que alguien más vinculado al negocio vea los beneficios que se obtendrían al implementarse. Tener una revisión independiente que ayude a definir las necesidades, contribuye con la seguridad, pero tiene costos que no siempre las Empresas están dispuestas a asumir.

Al hacer referencia a la seguridad, hay dos componentes en cuestión. Por un lado la parte más técnica, y por otro lo que tiene que ver con los controles, procedimientos y cultura de control de la organización; es decir, aun teniendo la mejor tecnología, si los empleados divulgan la información a la que tienen acceso, el problema va a estar presente. No sólo se debe invertir en tecnología, si no existe un plan ordenado de trabajo. Se considera una carga administrativa el hecho de cumplir con ciertos procedimientos que son importantes. Por tanto, las compañías quedan expuestas a un mal manejo o a una acción desleal, precisamente, por el manejo no apropiado de los datos personales por parte de los empleados, la falta de controles en los sistemas y la infracción a la Ley. Ante la existencia de evasión de datos, se tienen que tomar las medidas de seguridad técnicas para asegurarse que solo ingresen a esa información aquellos que deben hacerlo. Se deben establecer ciertas normas y políticas para saber que las personas que acceden, manejan adecuadamente esa información.

### **3.9. La previsión como estrategia.**

El cumplimiento de la Ley no se reduce a la publicación de un aviso de privacidad: se requiere de la implantación de controles que permitan salvaguardar la confidencialidad de los datos personales que se recaban y asegurar que solamente serán utilizados para los fines para los cuales fueron obtenidos. Las Empresas que están obligadas a cumplir con la LFPDPPP tienen la opción de adoptar un esquema de autorregulación que les permita obtener la certificación como se establece los parámetros de autorregulación publicados en el Diario Oficial de la Federación el 29 de mayo de 2014.

Debido a lo anterior, es importante que las Empresas cuenten con información específica y tengan acceso a la transferencia de conocimiento por parte de expertos en la materia, sobre los requisitos que deberán cumplir como son: cumplimiento de principios, creación e implementación de un documento de seguridad, además de contar con procedimientos adecuados para publicar el aviso de privacidad, para obtener el consentimiento de los titulares y para atender la solicitudes de derechos ARCO, así como en general conocimiento sobre los beneficios que se obtienen al dar un tratamiento adecuado a los datos personales, cumpliendo así con la regulación en la materia. Esta necesidad permitirá tomar ventaja frente a sus competidores.

Con lo anterior identifiqué la necesidad de contar con un esquema maduro y basado en las mejores prácticas, que sea adoptado por las Empresas para asegurar el

cumplimiento de la LFPDPPP. Un esquema que les permita, de forma sistemática, monitorear el cumplimiento y la adecuada aplicación de los controles establecidos para proteger la información, ya que el cumplimiento de la Ley requiere de la implementación de medidas administrativas, físicas y computacionales que permitan garantizar la seguridad de los datos, protegerla contra las amenazas externas y gestionar los riesgos asociados, garantizando la disponibilidad y confidencialidad.

Las organizaciones deberán asegurarse de que se mantienen en cumplimiento de lo estipulado por la Ley y, para ello, la adopción de las mejores prácticas y estándares del mercado les facilita la implementación de controles que se sujeten a las regulaciones y los requerimientos de cada organización, alineando las visiones de las distintas áreas de Tecnología, Legal y los Procesos de negocio. En materia de mejores prácticas y estándares en el mercado, ISO 27001 es un estándar para el establecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI), que cuenta con un conjunto de controles que se encargan de proteger la información desde distintos frentes: establecimientos de políticas de seguridad, clasificación de la información, procesos de autorización, acuerdos de confidencialidad, gestión de riesgos, relación con terceras partes, manejo de bienes, relación con el personal (antes, durante y después del empleo), manejo de áreas seguras y equipo de seguridad, cambios a la información, intercambio de información con terceros, control de acceso y cumplimiento con regulaciones, entre otros. Estos controles se alinean fácilmente a lo señalado por la Ley, incluyendo los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).

Por otra parte, ISO 20000 es un estándar que establece un conjunto de procesos que se alinean para establecer un Sistema de Gestión de Servicios de Tecnologías de Información (SGSTI), que permiten el monitoreo de los compromisos de Niveles de Servicio con los usuarios (tanto internos como externos), estableciendo un punto de contacto para dar atención a las solicitudes expresas de los mismos, que para el caso de la LFPDPPP apoya a garantizar los derechos ARCO. La seguridad de la información y la protección de los datos no se alcanza con un producto, sino a través de implementar un sistema que se encuentre inmerso en la organización, promovido por la dirección, con el que se haga consciente a todos los miembros sobre la importancia y sensibilidad de los datos e información que se manejan, así como establecer políticas que no dejen lugar a dudas de cuáles son los usos aceptables para cada tipo de información. Tanto ISO 20000 como ISO 27001 son estándares basados en un Sistema de Gestión, lo que implica que deberá

buscarse la mejora continua y el monitoreo contante de la eficiencia del sistema y los controles implantados. La certificación brinda a las organizaciones, la certidumbre de que la organización certificada cumple con el estándar o norma de referencia, que cuenta con un sistema interno de vigilancia que le permite identificar las desviaciones que pudieran presentarse y dar una respuesta rápida a los incidentes, así como la adopción de medidas para evitar su recurrencia. La Certificación de un SGSI garantiza que las Empresas cuentan con:

- Política sobre seguridad de información establecida.
- Identificación de los datos e información según su sensibilidad.
- Análisis y tratamiento de riesgos alineados a una metodología.
- Controles que garantizan la privacidad y acceso a la información.
- Mecanismos de control para actualizar los datos o los privilegios asociados a estos.
- Acuerdos de confidencialidad para intercambio de datos con terceras partes.
- Canales adecuados para el reporte de incidentes.
- Procedimientos de filtrado para la selección de proveedores.
- Controles y comprobaciones de seguridad para la selección del personal.

Si bien la implantación o certificación de algún estándar de gestión no garantiza el cumplimiento de lo estipulado por la LFPDPPP, sí proveen el referente más adecuado para dar cumplimiento a lo establecido en ésta. La certificación podrá solicitarse a cualquier organismo de certificación que esté acreditado en materia de protección de datos personales por una entidad de acreditación autorizada, a su vez, por la Secretaría de Economía. Las Empresas que hayan sido certificadas y que se encuentren inscritas en el Registro, además de cumplir con las obligaciones y principios previstos en la LFPDPPP, su reglamento y demás normativa, deberán cumplir con los alcances de la certificación que les fue otorgada y los requisitos que para ello le haya señalado el organismo de certificación. La Secretaría de Economía es la encargada de vigilar que el debido funcionamiento del sistema de certificación en materia de protección de datos personales y el IFAI la apoyará en la realización de esta tarea, solicitando tanto a la Secretaría, como a las entidades de acreditación y a los organismos de certificación que inicien investigaciones o procedimientos para suspender, revocar o cancelar, cuando proceda, las autorizaciones, acreditaciones otorgadas o certificados, cuando cuente con elementos suficientes para considerar que no se realizan las actividades de manera adecuada.

## CAPÍTULO CUARTO

### EL DERECHO EMPRESARIAL Y LA PROTECCIÓN DE DATOS PERSONALES Y SEGURIDAD DE LA INFORMACIÓN: HACIA UNA MODERNIZACIÓN DE LA ENSEÑANZA

#### **4.1. Necesidad e inclusión en la currícula de la Especialización en Derecho Empresarial.**

No queda ninguna duda de que la tecnología y las ciencias jurídicas no pueden ni deben mantenerse alejadas; de esta manera el Derecho y la Tecnología (además de otras disciplinas) convergen en el tratamiento de datos personales y las diversas figuras emergentes de la sociedad moderna, que constituyen los nuevos fenómenos sociales, como en el caso concreto lo es el Internet. Espejo de la sociedad, y a la vez su infraestructura tecnológica, que ha venido a ser el medio que permite el desarrollo de una serie de nuevas formas de relacionarse social y jurídicamente.

En una relación de total codependencia, la Internet al igual que otros productos de la tecnología, suscitan una serie de cambios históricos que no podrían haberse desarrollado, sin el avance tecnológico mismo, puesto que éste desarrollo supone una construcción social en torno a la tecnología, y que se ve reflejado no solo en el aumento del tráfico económico, sino también jurídico.

A lo largo de nuestro estudio he develado una de las formas concretas en las que el uso de la llamada “Tecnologías de la Información y las Comunicaciones” impacta sobre el orden regulador de conductas: el Derecho y la Protección de Datos Personales, e impone la necesidad de replantearnos el marco jurídico y los dogmas vigentes, los cuales no parecen adaptarse con docilidad a los nuevos fenómenos. En ese sentido, todo jurista que se precie de serlo, dejará de ser indiferente ante tal situación; en aras de dar paso al progreso, y orientará sus esfuerzos a promover reformas legales para avocarse a la comprensión y estudio de estos nuevos fenómenos globales.

El objetivo del presente párrafo, es plantear una propuesta concreta ante la necesidad de incluir en la Especialización en Derecho Empresarial la asignatura de *Protección de Datos Personales*, toda vez que en esta materia nuestro país aún se haya en una etapa muy incipiente, he querido desarrollar una enumeración superficial, de cuál es, a mi juicio, el contenido teórico y práctico que debe cubrirse para el efecto de que se imparta en nuestra Máxima Casa de Estudios, concentrando mi esfuerzo en algunas áreas de la

doctrina general del derecho que ante el avance científico y cultural que la sociedad ha experimentado, es necesario modificar y actualizar; ambas acciones en el marco de la modernidad y como una forma de enfrentar los nuevos desafíos en el mundo del Derecho, la academia y la profesión.

Así, al llegar a la recta final de la presente investigación, descubrí dos cosas que son fundamentales como aportación a la ciencia jurídica. La primera que mientras más se profundiza en la materia de protección de datos personales, me di cuenta que es importante implementarla en nuestro nivel académico, ya que no es un posible peligro, sino una verdadera afectación a un número cada vez más creciente de Empresarios.

En segundo lugar, es asombroso percatarse de los escasos esfuerzos en el sector Empresarial de nuestro país por tratar de estar al día con la legislación, tanto por los que exigen y producen grandes cambios en la sociedad (clase política), como por aquellos que nos preparan para hacer frente a tales cambios (académicos), lo que trae a la memoria el por qué la decisión de investigar sobre este actual tema. El deseo ha sido en todo momento contribuir a la adaptación al futuro, para enfrentar con mayor eficacia el cambio personal, social y jurídico que se está manifestando en la sociedad, siempre enmarcado en el objetivo cumplido de acrecentar la comprensión de la privacidad y el derecho a la autodeterminación informativa de las personas.

En ese orden de ideas, considero que la enseñanza de la asignatura de la Especialización en Derecho Empresarial en materia de Datos Personales debe iniciar cuanto antes, al efecto de garantizar que los profesionales que egresan estén preparados para afrontar los problemas reales que existen frente a la seguridad de la información.

#### **4.2. Enseñar la asignatura de Protección de Datos Personales y seguridad de la información en los actuales programas de estudio.**

Considero que el manejo de este tipo de apoyos no sólo resulta importante en la investigación, son incluso necesarias para el desempeño profesional, valor agregado que ahora como abogados se nos pide, al menos a nivel de Empresa. Uno de los compromisos fundamentales que se asume al momento de hablar de enseñanza de las ciencias jurídicas, es el de formar profesionales con capacidad para enfrentar al mundo globalizado de hoy con las herramientas adecuadas, es por ello, que en la confección de los programas de estudios se debe de tomar en cuenta, el avance tecnológico y científico de la sociedad. En ese sentido y como parte final de mi propuesta educativa, he querido dedicar unas cuantas

líneas para reflexionar acerca de la enseñanza de la seguridad de la información y datos personales.

También cuando se me plantea una asesoría para resolver un problema en materia de datos personales, se carecen de criterios de evaluación que van más allá de lo jurídico, como las probabilidades de éxito, por lo común atribuimos la contingencia del resultado a un tercero especialista. Nos sorprende cuando nos incorporamos a una organización en la que tenemos que estar encargados de la protección de datos personales, del resguardo de la información, en donde se exigen resultados, acreditación de avances, graficar y establecer de forma clara nuestros procesos.

Durante mi práctica profesional he tenido contacto con muchos abogados que ofrecen a todos los niveles sus servicios, para contratarse como abogados especialistas Empresariales internos o externos que no cumplen con las expectativas en el tema de Datos Personales, no tienen una visión global multidisciplinaria y ni económica. Consecuencia, de que nuestro país está en la etapa más precoz en materia de seguridad de la información y datos personales, se insiste, bastaría con incluirlas dentro del plan de estudios, toda vez que resulta necesario que los alumnos conozcan las fuentes de información que tienen a su alcance, máxime si se recuerda a los tan famosos *“mandamientos del abogado”* que me recuerdan la importancia de estudiar cada día de mi vida. Si bien nadie está en desacuerdo con que las universidades pueden y deben impulsar programas para mejorar la calidad de los especialistas que producen, impulsando la incorporación de una materia obligatoria para el efecto de que los futuros especialistas tengan una visión de los componentes principales y su contenido esencial, su vinculación con los principios y valores recogidos en los textos constitucionales, así como su relación con otros derechos.

Dicho en otras palabras, el enfoque que se pretende, tiene que proyectarse en la forma en cómo se debe entender y enseñar la cultura jurídica en materia de protección de datos, es decir, su pasado, presente y futuro.

Por otro lado, en relación al enfoque *social*, éste permitirá no sólo conocer el camino por el cual ha transitado la protección de los datos personales en el ámbito jurídico, el cual sin duda, ha sido originado a consecuencia del fenómeno tecnológico, sino que además, nos permitirá conocer esta nueva etapa de la humanidad, es decir, la nueva vida social influenciada por el creciente uso y desarrollo de la tecnología.

En relación con la perspectiva *social*, permitirá conocer las opiniones, prácticas o conductas que cada día se expresan en las redes sociales, tales como pensamientos, sentimientos, comentarios, fotografías y videos del quehacer cotidiano. Lo cual, en el pasado, sólo era conocida por uno mismo o por un grupo muy reducido de personas. Sin embargo, ahora la realidad es distinta, esto, como consecuencia de la incesante innovación científica y tecnológica, lo cual está significando un cambio que no sólo está afectando las vidas de las personas, sino también, su privacidad. Sin duda, la realidad a la que se enfrentan hoy las Empresas es aquella que tiene que ver con el uso y la implementación de la tecnología y la informática, la cual se está convirtiendo en un estilo de vida que ya no sólo es propio de los Estados, sino también lo está siendo para las personas.

Por ende, en relación con las Universidades y las Empresas, resulta preciso que los académicos adopten posturas a favor de la protección de los derechos, a fin de que pueda hacerse frente, particularmente, por aquellos órganos o instituciones encargados de tutelar la protección de los datos personales.

De ahí que, una cultura en materia de protección de datos debe atender básicamente a situaciones muy precisa, tales como, potenciar la educación, partiendo de los nativos digitales hasta los migrantes digitales, a fin de poder acercarlos a los riesgos, pero también, a los beneficios que la propia tecnología trae consigo misma. Más aún, concientizar a las Empresas acerca de la importancia de proteger los datos personales, no sólo con el establecimiento de un “aviso de privacidad”, a pesar de que sus características sean sencilla y contenga la información necesaria. Por lo que también es de suma importancia las medidas protectoras de la privacidad y la atribución de mayores responsabilidades a los proveedores de servicios.

Nos encontramos que más allá del estudio de lo que puede ser la informática jurídica, se requiere tener la aplicación de cómo utilizarla y no sólo a ella, también a todo lo que la tecnología aplica en nuestro desempeño. No existe una verdadera orientación del derecho Empresarial en materia de datos personales, los abogados crecen y se desarrollan en las Empresas. Lo complicado del derecho hace necesaria la especialización, como lo han llevado a cabo los médicos, que tienen bien identificadas y diferenciadas sus áreas, aunque su formación sea completa desde la universidad.

En definitiva y, atendiendo a la doble perspectiva de la educación en materia de protección de datos personales, de lo que se trata es hacer un uso adecuado y responsable

de la información propia y ajena, a fin de mantener la privacidad a salvo, evitando sanciones a las Empresas y que se convierta en una tarea difícil de cumplir ante la sociedad que cada vez es más globalizada y sin fronteras. Por lo que, sería ideal incluirlo como una asignatura en la Especialización de Derecho Empresarial.

#### **4.3. Propuesta para la incorporación de la asignatura de Protección de Datos personales en la Especialización de Derecho Empresarial.**

La propuesta tiene por objeto que el especialista en Derecho Empresarial conozca a profundidad la regulación jurídica en materia de Datos Personales y Seguridad de la Información, para lo cual he procurado centrarme en los fundamentos técnicos y jurídicos de la legislación en esa materia; el régimen jurídico de la información, elementos característicos de los delitos que se cometen por el mal uso obligando a toda persona física o moral que de tratamiento a bases de datos de clientes, proveedores o empleados, a contar con avisos de privacidad, implementar un departamento de protección de datos personales, así como aplicar medidas de seguridad acorde a la cantidad y naturaleza de los datos que se traten.

La asignatura permitirá conocer los aspectos clave de la Ley de Datos y brindará herramientas a los especialistas para que de forma práctica e inmediata, se lleven a cabo acciones tendientes a documentar las políticas de protección de datos.

Por lo que sin más preámbulos se pone a consideración la propuesta concreta para el estudio y enseñanza de lo que he llamado Datos Personales y Seguridad de la Información.

#### **Tema 1: Antecedentes y contexto actual de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) a nivel internacional y en México.**

- 1.1. Breves antecedentes históricos nacionales e internacionales.
- 1.2. El método y las fuentes del Derecho de las Nuevas Tecnologías.
- 1.3. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
- 1.4. Cultura de la privacidad.
- 1.5. Consecuencias de la ausencia o mala administración de datos personales.

#### **Tema 2: La Ley y su reglamento.**

- 2.1. La protección de datos: La protección de datos: significado. Los datos personales.
- 2.2. La LFPDPPP: Los principios de cumplimiento y deberes de seguridad y confidencialidad, transferencia de datos, autoridades y sanciones.
- 2.3. El reglamento: medidas de seguridad y auditoría de privacidad.

- 2.4. Departamento de Protección de Datos Personales y derechos de acceso, rectificación, cancelación y oposición (Derechos ARCO)

### **Tema 3: Documentos de cumplimiento.**

- 3.1. Características generales del aviso de privacidad.
- 3.2. Elaboración del aviso de privacidad.
- 3.3. Medidas compensatorias que contempla la Ley.
- 3.4. Contratos de remisión y transferencia de datos personales.
- 3.5. Documento de seguridad.

### **Tema 4: Implementación de la Ley de Protección de Datos Personales en Posesión de los Particulares en las Empresas.**

- 4.1. Capacitación.
- 4.2. Elaboración de documentos.
- 4.3. Departamento de protección de datos personales.
- 4.4. Medidas de seguridad.
- 4.5. Como documentar los procesos.

No está por demás advertir que lo que he intentado es hacer tan solo el esbozo de una visión sobre la enseñanza de Datos Personales. Lo importante es educar sobre el mundo técnico para aprender a servirse de él.

#### **4.4. Riesgos de las Empresas con la fuga de información.**

La fuga de información es un riesgo que debe ser considerado prioritario en el diseño de un esquema de seguridad de la información, teniendo en cuenta tanto los aspectos tecnológicos que involucra, como aquellos de gestión y educación para minimizar el mismo. En mi opinión, hoy día la gestión de la seguridad de la información supone una nueva ventaja competitiva para las Empresas que deberán tomar en cuenta y que brindará garantía, minimizará riesgos y costos, maximizando rentabilidad.

En el mundo digital actual el riesgo de brechas de seguridad, fugas o pérdidas de información nunca ha sido mayor. No sólo se ha multiplicado el volumen de información en circulación sino también el número de vías en las que la información puede ser almacenada y transferida sin el consentimiento del propietario. A pesar de la mayor concienciación sobre los riesgos y amenazas a la seguridad que encaran las Empresas y firmas profesionales de todo el mundo, las brechas de seguridad están aumentando y amenazando seriamente la solidez de los negocios y la privacidad de sus clientes.

Aun cuando los administradores de TI tienen a su disposición un extenso arsenal de soluciones de seguridad, los cibercriminales todavía atacan sistemas y roban valiosa información que pueden utilizar para fraude con tarjetas de crédito, robo de identidad y otras actividades ilícitas. Las Empresas de cada sector continúan informando de vulnerabilidades de seguridad y aun así, todavía permiten la exposición de su información más sensible y confidencial que enfrentan: redes sociales, dispositivos móviles, sistemas de información, seguridad en los sistemas de información y gestión de riesgos de terceros. En la actualidad, los empleados se llevan información cuando cambian de trabajo, poniendo así en riesgo la imagen e integridad de la compañía.

Para manejar esta situación, se deben evaluar las amenazas y el diseño de las políticas y procedimientos de las Empresas y que administran las redes sociales. Los dispositivos móviles, como los smartphones y las tablets, son cada vez mucho más frecuentes, los utilizan desde niños hasta adultos para acceder a las redes sociales, Internet y correo.

Los dispositivos móviles permiten acceder y distribuir información Empresarial desde cualquier lugar y en cualquier momento. Estos dispositivos ya se han convertido en parte integrante de la forma en que la gente realiza tareas, tanto en el trabajo como en sus vidas personales. La demanda creciente de información móvil por parte de la fuerza laboral está impulsando cambios en la manera en que las organizaciones apoyan y protegen el flujo de información.

Ahora que los dispositivos móviles tienen tantas aplicaciones (incluyendo datos corporativos), las organizaciones buscan determinar cuál es el impacto en la seguridad de información y cómo mejorar sus controles. Los riesgos son evidentes: pérdida o fuga potencial de importante información Empresarial, las limitaciones de seguridad dada la gama de dispositivos, software y sistemas operativos, hasta el robo de un dispositivo móvil debido a su pequeño tamaño. Las organizaciones también están migrando hacia los sistemas de información en la nube, para incrementar la efectividad de las iniciativas de sistemas de información, reducir costos, incrementar la flexibilidad operativa y generar una ventaja competitiva. Estas decisiones enfrentan riesgos y desafíos, los cuales son, a menudo, pasados por alto o no comprendidos.

Muchas Empresas han “tercerizado” algunas de sus actividades o procesos, desde centrales de llamadas para clientes hasta la planilla de remuneraciones, en la búsqueda de reducir sus costos e incrementar eficiencia. Sin embargo, los riesgos asociados no se pueden “tercerizar”; las Empresas retienen su responsabilidad, por lo que deben verificar que las políticas de terceros satisfagan sus propias normas de control.

Como parte del cambio se hace necesario dar a los especialistas en Derecho Empresarial herramientas para su desempeño profesional, en materias de datos personales y seguridad de la información, brindando una visión económica de costo-beneficio con la verdadera aplicación de la tecnología.

Existe una relación directa entre los problemas y contradicciones que vivimos en la práctica con nuestra falta de preparación, incluso parte de la corrupción se genera a través de ello, generando educación y verdadera cultura en materia jurídica, al menos si no se resuelve el problema de forma inmediata, se van generando la cultura para que en un futuro no lejano tengamos la posibilidad de ser parte del cambio para tener un mejor país.

Con una mejor preparación se pueden enfrentar los problemas de desempleo de baja remuneración creando oferta de empleo ya no demanda de empleos. En la medida que se asuma como abogados una responsabilidad social de generar resultados y beneficios para nuestros clientes, se incrementará nuestra participación y se mejorarán nuestras expectativas.

Pero como se pueden lograr esos resultados sin una visión distinta, sin herramientas para organizarnos, para demostrar el desempeño, para eficientar los recursos.

La publicidad negativa y las multas por infracciones al cumplimiento regulatorio, violaciones de seguridad y robo de datos que involucran a proveedores de procesos tercerizados han obligado a las Empresas a mejorar continuamente su programa y controles relacionados. Se deben aplicar los mismos estándares corporativos a los proveedores y asociados de negocios externos que a los propios empleados. Las Empresas, a menudo, adoptan un enfoque ad hoc, proveedor por proveedor, del riesgo de los procesos tercerizados.

Las Empresas que no cuentan con un programa implementado de gestión de riesgos de terceros pueden encontrarse frente a riesgos no solo financieros, sino de reputación,

cumplimiento y marca de la Empresa. A medida que las Empresas se dirigen a sus proveedores para que hagan más por ellos, se están volviendo más dependientes de terceros con quienes hacen negocios. Esto va mucho más allá de la viabilidad financiera del proveedor. En el entorno conectado de hoy, las acciones de un proveedor pueden tener consecuencias no deseadas para las Empresas que les compran.

A nivel de las Empresas, poco a poco se comprende mejor cuál es el riesgo de un ataque cibernético y sus posibles impactos. Sin embargo, muchas se sienten lejanas aún a estas amenazas, o solo están concentrando su seguridad o preocupación en un sector cuando en realidad tienen muchas vulnerabilidades.

Todo este panorama requiere que la seguridad de información sea parte de la agenda de los temas tratados en las Empresas con una perspectiva pragmática y racional en relación con los riesgos que se enfrentan y los presupuestos que se tienen para atenderlos. Particularmente, la Ley de Protección de Datos Personales establece acciones de control de índole legal, organizacional y técnico que las Empresas deben ejecutar para cumplir con lo requerido por la norma. Esta normativa establece, por parte del ente regulador, acciones de fiscalización y sanciones en caso de no cumplimiento.

Si bien mi propuesta no es, insisto, el remedio para regular la amplia gama de relaciones jurídicas que pueden suscitarse, considero que es una alternativa viable como parte de los esfuerzos para solucionar parte de la problemática apuntada a lo largo de este estudio.

En efecto, de adoptarse mi propuesta, se permitiría el esclarecimiento de una serie de conceptos jurídicos indeterminados que existen en la actual legislación dando paso a términos bien identificados y sobre todo susceptibles de ser aplicados en la vida cotidiana de las Empresas que, con independencia de su giro, den cabal cumplimiento con la Ley.

## CONCLUSIONES

Las bases que se plasmaron en los aspectos metodológicos referentes a: la justificación, la delimitación del objeto de estudio, el planteamiento de problema, su hipótesis y objetivo general, los cuales se establecieron al plantear originalmente esta investigación, en donde se señaló como objetivo de la tesina demostrar que no existía una conciencia generalizada en el Sector Empresarial acerca del cumplimiento de la Ley de Protección de Datos Personales, además de que no se habían explorado los alcances y consecuencias jurídicas. En virtud, de que el derecho a la protección de datos personales corresponde al derecho derivado de la vida privada y la intimidad de las personas que se vio amenazado con la aparición de las nuevas tecnologías porque modificaron la forma de almacenar y distribuir la información que debía ser resguardada. En la búsqueda del bien común, el derecho y la comunicación operan como herramientas indispensables para la creación de leyes y políticas públicas que establezcan límites a la libertad humana dentro de un orden y armonía, como principios básicos de toda sociedad. Por todo esto, es posible concluir que:

**Primera.** Los derechos humanos han tenido que evolucionar al paso de las circunstancias y las épocas. Es así como ahora se habla de una tercera generación de derechos relacionados con el uso de las nuevas tecnologías en una cultura posmaterialista que vislumbra la necesidad de reconocer los derechos y libertades mediante leyes específicas.

Gracias a los nuevos avances tecnológicos, estamos asistiendo a una "*desmaterialización de los actos jurídicos*" bien en **lato sensu** o en **stricto sensu**, ello sin importar donde se encuentran los objetos o los sujetos de las relaciones jurídicas. Lo que le interesa al usuario es llegar a ellos, obtenerlos de la forma más rápida, eficiente y económica posible; lo que nos lleva a afirmar que la computadora y demás medios de telecomunicación han cambiado las nociones de tiempo, espacio, distancia, fronteras y sin duda, de soberanía; así el mundo ya no es lo que era hace unos años, la "Era Digital" lo ha cambiado para siempre, y es el Derecho quien debe regular el sano desarrollo de esta evolución.

**Segunda.** El acelerado proceso de creación e implementación de la tecnología en la vida cotidiana, ha transformado, nuestro mundo de forma tal que en todos los aspectos de la cotidianeidad, se ha incorporado por lo menos algo de tecnología, ello sumado al hecho de que cada día surgen nuevas herramientas del progreso, que van cambiando más y más la forma en que nos comunicamos y por supuesto la forma en la que nos relacionamos con

nuestros congéneres; ahora todo es más rápido, más eficiente, pero no necesariamente mejor, **y no necesariamente más seguro.**

**Tercera.** En efecto, hablar de seguridad en las redes de telecomunicación, se presta para diferentes interpretaciones, al técnico importará el desarrollo de los sistemas que prevengan la intromisión de intrusos no deseados al interior de un sistema, pero a los especialistas del Derecho Empresarial, se nos plantean otros retos, como por ejemplo, el garantizar el derecho a la privacidad de nuestros clientes, empleados y proveedores, o bien la libertad de expresión y otras libertades civiles que hoy por hoy, en el marco del ordenamiento jurídico fundamental, los gobiernos del mundo solo pueden garantizar en parte, pues el desarrollo de las nuevas tecnologías si bien permite el progreso, ha traído aparejado una serie de problemas técnico- jurídicos, por falta de una regulación y aplicación adecuada.

**Cuarta.** Surge por tanto, la necesidad de crear nuevas normas destinadas a una nueva sociedad: la de la información; formada por comunidades de personas de todo el mundo y que se desenvuelven en un espacio que existe y se desarrolla a su propio ritmo, pero únicamente en términos de valores binarios, que tal vez para nosotros los seres humanos ordinarios no signifiquen mucho, pero que transmitidos a través de redes de computadoras, puede traducirse en el simple saludo de un amigo distante, o bien, en el pago del negocio más grande que cualquier Empresa pudiera haber realizado y que el mal uso que se pueda dar a sus datos personales puede ocasionar sanciones exorbitantes que pueden poner en riesgo la estabilidad de la Empresa.

Lo anterior tiene relevancia, debido a que no existe una sola área de la vida humana que se esté viendo afectada de manera particular, sino que la cultura en general está viviendo una de las revoluciones más grandes de nuestra historia y que solo podría ser comparada pálidamente con la revolución industrial de principios de siglo.

**Quinta.** La Revolución Industrial no solo abrió el camino al ejército de máquinas que sirvieron para mejorar la vida del Hombre, sino que a la par dio surgimiento a los movimientos obreros, a los movimientos feministas y en general a un drástico cambio en el pensamiento de la sociedad, circunstancia que es muy parecida a la que estamos viviendo. Por tanto, si los movimientos político-culturales de principios de siglo dieron origen al surgimiento de los derechos de los trabajadores, o la igualdad de los derechos de la mujer, no es extraño pensar que la revolución tecnológica dé paso a una serie de derechos

dirigidos precisamente a los usuarios de la tecnología que no solo cambió su forma de vivir, sino también de pensar.

**Sexta.** Se necesitan de nuevas normas jurídicas para regular situaciones que el Derecho antes no pudo prever (porque eran materialmente impensables) entonces, se vislumbra también la necesidad de la creación de una nueva rama del Derecho que se encargue de estudiar bajo una óptica única, estas disposiciones legales emergentes y que además impulse el desarrollo de protección y tecnologías de la información sin que ello implique sacrificar los derechos heredados del hombre; por lo que puedo afirmar, que si el desarrollo de las nuevas tecnologías es la solución más eficaz a necesidades previas, es también el principio de nuevas necesidades, que requieren de una solución jurídica.

El reto, en este caso, es cumplir con la normatividad para hacer un uso apropiado de toda esta información que, desasociado del particular, puede servir para la investigación o para la academia. Está muy ligado con la ética profesional del médico, aún para determinar los casos en los que debe optar por denunciar alguna situación que pudiera poner en riesgo la salud pública para establecer cercos sanitarios.

**Séptima.** Otro sector muy vulnerable es el educativo. Contiene información de alrededor 25 millones de estudiantes en México, además del registro oficial de documentos académicos y de certificación. Se trata de una tercera parte de la población mexicana cuyas bases de datos están inscritos en el Sistema Persona del IFAI. Lo que debería garantizar la información depositada en las escuelas privadas para evitar que no sea utilizada con otros fines más que los establecidos.

En el sector de las telecomunicaciones, bajo el pretexto de que la Ley Federal de Telecomunicaciones sólo establece la confidencialidad de la información transmitida mediante las redes y servicios de telecomunicaciones, salvo las excepciones indicadas, algunas Empresas del sector privado han incurrido en mal uso de la información de sus clientes sin recibir ninguna sanción.

Es lamentable cómo las mismas Empresas violan sus propias condiciones de seguridad por cumplir con otros intereses, en detrimento de la confianza que los usuarios depositan en ellas, que aún y con la ley en vigor los derechos de las personas su privacidad

se ve invadida por terceros sin su consentimiento, y no es utilizada para los fines para la que fue autorizada.

El comercio electrónico requiere la confianza de los usuarios de Internet para que utilicen este medio. La información personal es lo más valioso que las compañías tienen en su poder, por esto es necesario garantizar su seguridad en la red. Cuando las personas saben que sus datos son debidamente resguardados confían más en hacer uso de Internet para realizar sus operaciones. Por esto es importante que las Empresas apliquen la autorregulación como un mecanismo que dé confiabilidad, además de cumplir lo dispuesto por la ley, lo que se reflejará en el incremento de sus ingresos.

**Octava.** Es necesario entender que todo sistema constitucional de derechos fundamentales debe proteger la libertad siempre y cuando no afecte a terceros. De esta manera, el tema de la protección de datos personales se confronta ante ciertas libertades y derechos establecidos, tal es el caso de la libertad de expresión, necesaria para la creación de la opinión pública; el derecho a la información como un derecho fundamental, indispensable para la toma de decisiones como parte del proceso de la comunicación; el derecho de acceso a la información pública que otorga a los ciudadanos la garantía de acceder a la información que está en manos del gobierno para conocer su forma de trabajo, el manejo de recursos públicos, sus resultados y desempeño; el derecho a la vida privada que otorga libertad de creencias, libertad ideológica, derecho a la inviolabilidad del domicilio, etcétera, o el derecho a la intimidad, ámbito que no puede ser invadido por la difusión de mensajes informativos.

Adicionalmente se planteó que las normas jurídicas destinadas a regular el uso y aprovechamiento de las nuevas tecnologías no deben ser estudiadas por la ciencia del Derecho como pequeños fragmentos de otras ramas del conocimiento jurídico, o limitándose a hacer algunos breves comentarios dentro de otras asignaturas, sino que deben verse como un verdadero campo de estudio independiente, con sus propias normas y principios distintos de las demás materias.

**Novena.** El avance tecnológico acentuó el peligro que corre la intimidad de las personas porque facilita la intromisión de terceros en la información que se desea resguardar tal como domicilio, registros privados, conversaciones telefónicas, datos financieros, ideología, etcétera. Por estas razones es necesario cumplir las leyes y políticas que protegieran la

información personal aunque surgiera cierta tensión entre derechos, pero su regulación se ha convertido en un elemento indispensable para las democracias modernas.

El tema que está muy de moda actualmente es el de las redes sociales. El dilema de la seguridad en ellas en parte consiste en establecer mecanismos de prevención mediante la educación de los usuarios para que aprendan a autoproteger su información que suben a la red, pero también corresponde a las leyes velar por que estos espacios ofrezcan políticas de privacidad que garanticen el uso adecuado de la información para salvaguardar la integridad física y moral de las personas.

**Undécima.** La autorregulación es indispensable porque si las Empresas implementan voluntariamente mecanismos que garanticen cumplir con la ley, además de evitar el riesgo de la sanción, adquieren el beneficio de la confianza de sus clientes. El derecho comparado ha servido para esclarecer la relación que existe entre los medios de información y el derecho a la protección de datos personales. Al igual que el acceso a la información, existe también el derecho que tienen los medios de comunicación de informar, cuya actividad está amparada constitucionalmente.

Se trata de derechos opuestos, aunque también es cuestión de ética del periodista que en ocasiones debe guardar la confidencialidad de su fuente para evitar algún peligro sobre su persona o que sea expuesto de forma injusta. No obstante, el derecho a la protección de datos personales no debe ser pretexto para negar información que la ciudadanía debe conocer cuando el periodista considera su obligación difundirla, y resulta más difícil todavía intentar proteger datos privados cuando se trata de personas que por su actividad son figuras públicas, como lo menciona la jurisprudencia.

**Duodécima.** Para que la aplicación del derecho a la protección de datos personales en México sea lo más exitosa posible deben intervenir diferentes factores: una ley eficaz, preventiva y sancionadora; un órgano garante; mecanismos de autorregulación de las Empresas e instituciones; ética profesional de quienes trabajan directamente con los datos; enseñanza para que las personas conozcan el derecho, lo apliquen y hagan uso consciente de su información personal; cooperación entre naciones para seguir realizando foros y espacios que abran nuevas vertientes y den nuevas aportaciones al derecho que puedan ser llevadas a la práctica con el fin de que no se queden meramente en la teoría y, finalmente, corresponsabilidad de todos los actores involucrados. De esta manera podrá lograrse la

armonía necesaria para que los diversos sectores realicen sus actividades dentro del marco de la protección del derecho a la protección de datos personales.

**Decimotercera.** Considero que cada uno de los problemas que han surgido como consecuencia del incumplimiento a la Ley Federal de Protección de Datos Personales, merece la posibilidad y necesidad de incluir en la curricula de la Especialización de Derecho Empresarial, con ello se podrá estudiar a profundidad los nuevos problemas jurídicos que están surgiendo como consecuencia de la tecnología, y es que el problema no es una cuestión meramente local y de legislación interna, sino que gracias al desarrollo de inventos como el Internet y otros medios masivos de comunicación, los problemas derivados de la incorporación de la tecnología a la vida cotidiana, trascienden fronteras, sin que necesariamente este sea un campo de estudio exclusivo del Derecho internacional privado, o público en su caso.

**Decimocuarta.** En una adecuación a la investigación, debo precisar que uno de los problemas que me pareció que requiere de atención inmediata de nuestros juristas y legisladores por igual, es precisamente el concepto de “mensaje de datos” y que en la legislación comercial señala que la información generada, recibida, archivada o transmitida por medios electrónicos, ópticos o similares, pudiendo ser entre otros, el Intercambio Electrónico de Datos (EDI), el correo electrónico, el telegrama, el telefax, el telex, etcétera, es hoy por hoy, uno de los conceptos legales que con el paso del tiempo continuará adquiriendo mayor relevancia tanto para laicos, como para los estudiosos del derecho Empresarial, sin embargo poco se ha hecho por estudiar su alcance y contenido.

**Decimoquinta.** Debe puntualizarse que se requiere atención al fenómeno tecnológico aquí desarrollado, y por igual, de abogados Empresariales y funcionarios judiciales, dado que las normas del Derecho y sus principios, necesitan en el marco de la dogmática jurídica, ser correctamente interpretados para determinar si se aplican o no a los diferentes sectores de Empresas en el marco de la modernidad impuesta por la tecnología, ello en consideración de que se necesita empezar a replantear las figuras de la doctrina clásica del Derecho, para que así se incorpore a la especialidad, el manejo de términos absolutamente desvinculados de las clases tradicionales de la carrera del Derecho; en ese contexto se escuchara cada día con más frecuencia conceptos como: autenticidad, integridad, no repudio y confidencialidad de las comunicaciones, y que a decir de los nuevos estudiosos del Derecho, representan los elementos necesarios para la existencia del cumplimiento de la ley.

**Decimosexta.** En ese orden de ideas el objetivo de esta tesina, fue esbozar a la luz de una necesidad e inclusión en la especialización de Derecho Empresarial la materia de Protección de Datos Personales, como consecuencia de lo que he presentado en esta investigación y considerando la naturaleza y alcance jurídico. La protección de datos personales es un tema vital en la actualidad y es una garantía para el desarrollo de cualquier actividad Empresarial. De los casos particulares expuestos sobre algunos sectores expuestos, es posible concluir que:

Como he comentado con anterioridad, las sociedades de información crediticia son la excepción de la ley que no tiene una explicación técnica sino de intereses y presiones políticas y sectoriales. La información que éstas manejan es alimentada por toda clase de instituciones financieras, compañías de tarjetas de crédito, telecomunicaciones, arrendadoras, autos, tiendas departamentales y demás Empresas comerciales. Son datos de millones de usuarios que deberían tener toda la protección que ofrece la nueva ley de particulares y no sólo la cobertura de su ley sectorial.

Si esta información no recibe el tratamiento adecuado puede representar un serio riesgo para las Empresas porque el cruce de datos fácilmente permite realizar perfiles completos que den a conocer los hábitos de consumo de las personas y, como consecuencia, podrían ser víctimas de secuestro o fraude, o recibir propaganda de productos o servicios no deseados mediante llamadas telefónicas, correo electrónico o correspondencia a domicilio.

**Decimoséptima.** Es un hecho que para que las Empresas den observancia a la ley deberán considerar la asignación de presupuesto para seguridad de TI y hacer de la protección de información una práctica común en la operación del negocio. Con frecuencia la responsabilidad de asegurar el cumplimiento de las regulaciones recae en los profesionales de TI, sin embargo, para que éste sea adecuado tendrán que estar involucrados diversas áreas de la Empresa, empezando por los dueños de procesos del negocio, el área legal, Recursos Humanos, Sistemas y TI. No hay que olvidar que la falla en este sentido puede traer serias consecuencias, incluyendo multas sustanciales y demandas legales que afectarán directamente la salud financiera de la Empresa.

Consecuencia a lo anterior, todas las Empresas deben adaptarse a la legislación teniendo en cuenta que deben relacionar por un lado, los derechos que poseen los

ciudadanos sobre el uso y tratamiento de sus datos y, por otro, las medidas y técnicas que se deben establecer para garantizar la seguridad de la información.

**Decimoctava.** Como consecuencia de todos los avances científicos y del surgimiento de los problemas jurídicos apuntados, considero que se impone la necesidad e inclusión en la currícula de la Especialización en Derecho Empresarial. La alta tecnología puede ser vista por el jurista de la era digital desde dos perspectivas, por un lado representa una herramienta que hay que aprender a usar y por la otra es una actividad humana que requiere ser regulada o reglamentada de alguna manera, por lo que los profesionales del Derecho de nuestro tiempo no se pueden desconocer las implicaciones existentes entre la tecnología y el Derecho. Se debe reconocer que aún se está en la etapa más precoz en materia de Protección de Datos personales.

**Decimonovena.** Existen dos campos de acción que considero básicos para dar solución a los problemas de falta de seguridad jurídica generados como consecuencia del uso de las nuevas tecnologías (por lo menos hasta ahora), de tal suerte que hay el imperativo de dar cumplimiento con los planes y programas propuestos para las Empresas y la necesidad e inclusión de la materia en la especialización de Derecho Empresarial.

Tales acciones propositivas no están peleadas, ni deben tomar rumbos separados, su vinculación es estrecha, y su concreción obliga a tomar en cuenta la realidad socio-jurídica para sembrar en los especialistas Empresariales la semilla que permita competir eficazmente en el mercado laboral.

**Vigésima.** Así mi propuesta, se soporta en un estudio doctrinario que revela por un lado los problemas jurídicos derivados de la protección de datos personales y seguridad de la información, pero además promueve el estudio y comprensión de esos problemas. El estudio de los problemas jurídicos producto de la evolución científica y cultural solo tiene una solución que es la amalgama de la educación, por lo que a la par del desarrollo de las nuevas tecnologías, debe irse desarrollando el estudio de las normas destinadas a su aplicación, ello es, mientras la sociedad avanza, el estudio de las normas que ella misma se otorga debe irse dando simultáneamente.

**Vigésima Primera.** Por esta razón, el trabajo de investigación insiste en la conveniencia de que las Empresas deben clarificar los alcances y servir de apoyo para que ajusten sus

actividades cotidianas en el tratamiento o manejo de datos personales con lo que dispone la normatividad aplicable a la materia. Ante el escenario de la LFPDPPP, las Empresas tienen una mayor responsabilidad de resguardar la información de sus clientes, pero más allá de este requerimiento legal, se abre una oportunidad de negocio para capitalizar el valor de contar con datos maestros, seguros y confiables para utilizarlos de manera correcta en su toma de decisiones.

En un mundo cuya economía gira en torno a la información, es de extrema importancia contar con una legislación que proteja los datos personales. En México esa necesidad es clara y ahora con la LFPDPPP los registros médicos, financieros, educativos de los titulares deberán ser tratados y protegidos de manera adecuada.

Descritas así algunas conclusiones en el contexto de mi proyecto inicial por lo que hace al objetivo, sigo con toda la posible fidelidad, la problemática del caso, y de sus respectivas hipótesis que justificaron a la investigación. Por tanto, queda a criterio de los futuros lectores considerar mis propuestas y, será el tiempo y la propia evolución de la cultura humana, quien resolverá a mi favor.

## FUENTES DE CONSULTA

### A. BIBLIOGRÁFICAS

1. CANTORAL DOMÍNGUEZ, Karla, ***Derecho de Protección de Datos Personales de la Salud***, Liber Iuris Novum, México, 2012.
2. FERRER, E., ***Comunicación y Comunicología***, México, D.F., Ed., Eufesa, México, 1982.
3. GÓMEZ-COTERO, José de Jesús, ***Medios electrónicos, cumplimiento de obligaciones fiscales y mercantiles***, Dofiscal Editores, México, 2010.
4. GÓMEZ, A. y ORNELAS, L., ***Protección de Datos Personales en México: el caso del Poder Ejecutivo Federal***. México: UNAM.
5. MALVIDO, Adriana, ***Por la vereda digital***, CONACULTA, México, 1999.
6. MARTÍNEZ-ALFARO, Joaquín, ***Teoría de las obligaciones***, Porrúa, 4ª Ed., México, 1997.
7. MONZÓN, Cándido, ***Opinión pública, comunicación y política***, Madrid, Ed., Tecnos, 1996.
8. MUÑOZ, Luis, ***Derecho comercial, contratos***, Tipográfica Editora Argentina, Buenos Aires Argentina, 1960.
9. NIKLAS, Luhmann. Traducción Gaytán Alcalá Felipe. ***Notas Críticas. Teoría de sistemas, la autoobservación de la sociedad moderna***. Editorial Alianza. 2002.
10. ORNELAS NÚÑEZ, Luis, ***Curso Ley Federal de Protección de Datos Personales de los Particulares y sus Reglamento***, Tirant Lo Blanch Formación, México, 2012.
11. ORNELAS NÚÑEZ, L. y LÓPEZ AYLLÓN, S., ***La recepción del Derecho a la protección de datos en México: Breve descripción de su origen y estatus legislativo***”, en *Protección de datos personales: Compendio de lecturas y legislación*, Instituto Federal de Acceso a la Información Pública, México 2010.
12. PIÑAR MAÑAS, José Luis y ORNELAS, Lina, ***La Protección de Datos Personales en México***, Tirant Lo Blanch, México, D.F., 2013.
13. PRICE, Vicent, ***Opinión Pública***, México, D.F., Ed., Paidós, México, 1994.
14. PFAFFENBERGER, Bryan, ***Internet In Plain English***, Ed. MIS Press, New York, Estados Unidos, 1994.
15. TÉLLEZ-VALDÉS, Julio, ***Derecho informático***, México, Ed., Mc Graw-Hill, 2ª ed, 2000.
16. VILLANUEVA, Ernesto. Centro de Investigaciones Jurídicas Udlap. Puebla, México- Entrevista personal. Septiembre-2010.
17. WALTON, Dominique, ***Internet y después qué?*** Ed. Gedisa, Barcelona España, Colección: El mamífero Parlante, 2010.

## B. NORMATIVAS

1. Constitución Política de los Estados Unidos Mexicanos (Publicada en el Diario Oficial de la Federación el 5 de febrero de 1917. Última reforma publicada Diario Oficial de la Federación 7 de julio de 2014). Disponible en <http://www.diputados.gob.mx/LeyesBiblio/index.htm>
2. Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Nueva Ley publicada en el Diario Oficial de la Federación el 5 de julio de 2010). Disponible en <http://www.diputados.gob.mx/LeyesBiblio/index.htm>
3. Ley Federal de Protección al Consumidor (Nueva Ley publicada en el Diario Oficial de la Federación el 24 de diciembre de 1992. Última reforma publicada Diario Oficial de la Federación 4 de junio de 1992). Disponible en <http://www.diputados.gob.mx/LeyesBiblio/index.htm>
4. Ley Federal de Radio y Televisión (Nueva Ley publicada en el Diario Oficial de la Federación el 19 de enero de 1960. Última reforma publicada Diario Oficial de la Federación 11 de abril de 2006). Disponible en <http://www.diputados.gob.mx/LeyesBiblio/index.htm>
5. Ley Federal del Derecho de Autor (Nueva Ley publicada en el Diario Oficial de la Federación el 24 de diciembre de 1996. Última reforma publicada Diario Oficial de la Federación 17 de marzo de 1996). Disponible en <http://www.diputados.gob.mx/LeyesBiblio/index.htm>
6. Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Nuevo Reglamento publicado en el Diario Oficial de la Federación el 21 de diciembre de 2011). Disponible en <http://www.diputados.gob.mx/LeyesBiblio/index.htm>

## C. ELECTRÓNICAS

1. AGRELA ROMERO, Belén, ***La acción social y las mujeres inmigrantes: ¿Hacia unos modelos de intervención?*** [En línea] <<http://rabida.uhu.es/dspace/bitstream/handle/10272/170/b15124794.pdf?sequence=1>>
2. CALDERÓN, M. (2010). ***La protección de datos en el sector de las telecomunicaciones***. Panel presentado en el VIII Encuentro Iberoamericano de

Protección de Datos Personales en septiembre de 2010, organizado por el IFAI, México. Versión estenográfica disponible en <http://viiiencuentroiberoamericano.ifai.org.mx/index.php/material>

3. CARRASCO-RODRÍGUEZ, Alberto, *et al.*, **Historia de la informática y metodología científica** [En línea] Biografías de Personajes Científicos e Informáticos < <http://usuarios.lycos.es/hv1102/hollerith.html>>
4. CISCOMANI, Francisco, (2010). **Apertura del VIII Encuentro Iberoamericano de Protección de datos personales**. 29 de septiembre de 2010. Organizado por el IFAI, México. Versión estenográfica disponible en <http://viiiencuentroiberoamericano.ifai.org.mx/index.php/material>
5. GRANERO, Horacio R., **El impacto de las nuevas tecnologías en el derecho**. [En línea] Instituto de Informática Jurídica de la Universidad del Salvador. (El derecho y la Alta tecnología) < <http://www.salvador.edu.ar/ua1-4-hg.htm>>
6. INE, **Manifestación de Protección de Datos Personales recabados por Registro Federal de Electores** [En línea]: <http://www.ine.mx/archivos2/portal/credencial/datosPersonales.html/>>
7. INEGI, **Historia de la informática**, [En línea]: Ciberhábitat Ciudad de la Información. Diciembre 2000, Actualizado Agosto 2001. <[http://ciberhabitat.gob.mx/museo/historia/texto/texto\\_sigxx.htm](http://ciberhabitat.gob.mx/museo/historia/texto/texto_sigxx.htm)>
8. Instituto Federal de Telecomunicaciones, **IFT-1 Licitación de dos cadenas de televisión radiodifundida digital** [En línea]: <http://portalanterior.ift.org.mx/iftweb/industria-intermedia/unidad-de-sistemas-de-radio-y-television/licitaciones-en-curso-radio-y-television/licitacion-ift-1/>
9. LAHERA, Eugenio P., **Política y Políticas públicas**. [En línea] <<http://cgpp.app.jalisco.gob.mx/images/politicaspublicas.pdf>>
10. PARRA, R. **La protección de datos en el sector de las telecomunicaciones**. Panel presentado en el VIII Encuentro Iberoamericano de Protección de Datos Personales en septiembre de 2010, organizado por el IFAI, México. Versión estenográfica disponible en <http://viiiencuentroiberoamericano.ifai.org.mx/index.php/material>
11. PIÑA-LIBIEN, Hiram Raúl, **Proyecto: Base bibliográfica de derecho informático**, [En línea] Comunidad Alfaa-REDI. <<http://www.alfa-redi.org/base/base-sp.asp>>.
12. PRENAFETA-RODRÍGUEZ, Javier, **Protección de datos de carácter personal e Internet**, [En línea]: Artículos doctrinales: Derecho Informático, agosto 2002, <[http://noticias.juridicas.com/areas/20-Derecho%20Inform%20E1tico/10-Art % Edcuos /200208-55561531610232111.html#foot11](http://noticias.juridicas.com/areas/20-Derecho%20Inform%20E1tico/10-Art%20Educos/200208-55561531610232111.html#foot11)>
13. RÍOFRIO, Juan Carlos, **Ecuador: La pretendida autonomía del derecho informático**. [En línea] Alfa - Redi: Revista de Derecho Informático <<http://www.ub.es/biblio/citae-e.htm>>
14. SABOGAL-RUEDA, Alexander, Conceptos Generales de Telemática. [En línea] <[www.uninet.edu/ummet/conferencias/AlexSabogal/tele2.ppt](http://www.uninet.edu/ummet/conferencias/AlexSabogal/tele2.ppt)>

## D. OTRAS

1. **Cámara de Comercio, Servicios y Turismo de Monterrey, El impacto de las nuevas tecnologías en las Empresas,** [En línea] <<https://comisionlegalcanaco.wordpress.com/2012/03/20/sociedades-de-informacion-crediticia-excentas-de-las-obligaciones-de-privacidad/>>
2. **DEMERS F. y LAVIGNE, A., La comunicación pública: una prioridad contemporánea de investigación.** Novena Época, núm. 7, enero-junio, 2007.
3. **Dictamen de las Comisiones Unidas de Gobernación y de Estudios Legislativos,** a la Minuta con Proyecto de Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Este Dictamen tiene fecha del 27 de abril de 2010 y está disponible en la página de la Suprema Corte de Justicia de la Nación, en la liga <http://www2.scjn.gob.mx/red/leyes/>, al acceder al apartado “Procesos Legislativos” de la LFPDPPP.
4. **Dictamen con proyecto de decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de Particulares**
5. **El First Virtual Bank,** es el proyecto conjunto con el banco First USA que permite a los compradores de la Internet o World Wide Web abrir cuentas centrales utilizando tarjetas de crédito, de ésta forma los compradores pueden usar sus números cuenta para hacer compras en cualquiera de un número de comercios participantes. Vid. Hutchinson Encyclopedya [En línea] Dictionary Computers [USA] <<http://www.tiscali.co.uk/reference/dictionaries/computers/data/m0051242.html>>
6. **Escobedo, Juan Francisco, Movilización de opinión pública: El caso del Grupo Oaxaca y la Ley Federal de Transparencia y Acceso a la Información Pública, en México, UIA,** Revista Iberoamericana de Comunicación, núm. 3, otoño-invierno. 2002.
7. **Espinar Ruiz, Eva; LÓPEZ Fernández, Cristina, Jóvenes y adolescentes ante las nuevas tecnologías: percepción de riesgos,** Athenea Digital. Revista de Pensamiento e Investigación Social. Núm. 16 (otoño 2009) ISSN 1578-8946.
8. **Estándares Internacionales sobre Protección de Datos Personales y Privacidad (Resolución de Madrid),** adoptada durante la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada el 5 de noviembre de 2009 en Madrid. La Resolución de Madrid está disponible, en español, en la siguiente dirección de Internet: [http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31\\_conferencia\\_internacional/estandares\\_resolucion\\_madrid\\_es.pdf](http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf)
9. **Fuente: 13a Encuesta Global de Seguridad de la información (EGSI) y comparativo México. Perpectivas sobre los riesgos de TI,** [En línea]: [http://www.ey.com/Publication/vwLUAssets/Seguridad\\_de\\_la\\_informacion\\_en\\_un\\_mundo\\_sin\\_fronteras/\\$FILE/Seguridad\\_de\\_la\\_informacion\\_en\\_un\\_mundo\\_sin\\_fronteras.pdf](http://www.ey.com/Publication/vwLUAssets/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras/$FILE/Seguridad_de_la_informacion_en_un_mundo_sin_fronteras.pdf)

10. **Fundación para la Libertad de Expresión.** Consulta No. 17. Preguntas frecuentes. En línea <http://www.fundalex.org/preguntas-frecuentes-3.php>.
11. **González, Luz (2010).** Tepito vende bases de datos oficiales. El Universal en línea. <http://www.eluniversal.com.mx/primera/34792.html>>
12. **José Ángel Cabrera y Nantzin Saldaña,** 24 horas el Diario sin límites, **Peña Nieto promulga leyes telecom; anuncia Nueva cadena de TV pública.** [En línea]: <http://www.24-horas.mx/pena-nieto-promulga-leyes-telecom-anuncia-nueva-cadena-de-tv-publica/>
13. **Apud, MALVIDO, Adriana,** Por la vereda digital, México, CONACULTA, 1999.
14. **Marco de Privacidad de APEC.**
15. **Tesis aislada No. 165820.** Derechos al honor y a la privacidad. 1a. CCXIX/2009 Primera Sala. Novena Época. Semanario Judicial de la Federación y su Gaceta. Tomo CCXIX/2009, Diciembre de 2009.
16. **Tesis aislada No. 172912.** Responsabilidad de periodistas y medios de comunicación. I.3o.C.607 C. Primera Sala. Novena Época. Semanario Judicial de la Federación y su Gaceta. Tomo XXV, Marzo de 2007.
17. **Tesis aislada No. 164987.** Medios de comunicación. 1a. XLV/2010. Primera Sala. Novena Época. Semanario Judicial de la Federación y su Gaceta. Tomo XXXI, Marzo de 2010.

## G L O S A R I O

**APEC:** Foro de Cooperación Económica de Asia Pacífico.

**ARCO:** Derechos de Acceso, Rectificación, Cancelación y Oposición.

**ATTACHMENT:** es el término anglosajón que se emplea para referirse a los archivos que se adjuntan a un mensaje de correo electrónico, en nuestro país es común usar esta expresión o sustituirla por la frase “archivo adjunto”.

**BM:** Banco de México.

**CNBV:** Comisión Nacional de Bancaria y de Valores.

**CNDH:** Comisión Nacional de Derechos Humanos.

**CRACKER:** Es una especie de Hacker cuya ocupación es buscar la forma de entrar en sistemas y encontrar las fallas de seguridad de los programas.

**EGSI:** Encuesta Global de Seguridad de la información.

**ENDUTIH:** Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información.

**FIRST VIRTUAL BANK:** Es el proyecto conjunto con el banco First USA que permite a los compradores de la Internet o World Wide Web abrir cuentas centrales utilizando tarjetas de crédito, de ésta forma los compradores pueden usar sus números cuenta para hacer compras en cualquiera de un número de comercios participantes.

**FDT:** Flujo de Datos Transfronterizos.

**HACKERS:** Individuos altamente conocedores de los sistemas informáticos que se infiltran a los mismos con el objetivo de hurtar información o simplemente por el reto que representa la infiltración; en la mayoría de las ocasiones sus actividades se limitan a la protesta o las bromas pesadas, sin embargo en ocasiones pueden llegar a ocasionar serios daños a los sistemas que son víctimas de sus ataques.

**HTML:** son las siglas en inglés que sirven para referirse a Hiper-Text Markup Lenguaje que aunque no se considera realmente un lenguaje de programación, la mayoría de los documentos en el Internet se escriben utilizando este sistema de etiquetas, originalmente se pensó que era un sistema seguro de distribución a través de la Red, debido a que solo podía indicar a los ordenadores la forma en la que se debía de representar un determinado texto, sin embargo hoy en día ya es posible difundir un virus informático haciendo uso de este lenguaje.

**IBM:** International Business Machines.

**IFAI:** Instituto Federal de Acceso a la Información.

**IFT:** Instituto Federal de Telecomunicaciones.

**INE:** Instituto Nacional Electoral.

**INEGI:** Instituto Nacional de Estadística y Geografía.

**JAVA:** Es un lenguaje de programación orientado a objetos muy parecido al diverso C++, es comúnmente utilizado por programadores y diseñadores de la Red para la telecarga o ejecución a distancia de programas en la computadora del usuario del sitio y fue desarrollado por Sun Microsystems.

**KB:** Significa la unidad de medición de la capacidad de memoria de los equipos informáticos está dada en Bits. Un bit representa un dato o un carácter almacenando al interior de la computadora, sin embargo al ser los bits, unidades tan pequeñas de medición en comparación con la cantidad de información que puede llegar a almacenarse en un ordenador, normalmente la capacidad de memoria se expresa en Bites un múltiplo de la unidad que contiene aproximadamente 1024 bits y no es el único múltiplo de esta unidad que existe pues también tenemos al Kilo Bite (Kb) el Mega bite (Mb) y el Giga Bite (Gb).

**LFPDPPP:** Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

**LEGIPE:** Ley General de Instituciones y Procedimientos Electorales.

**NETIQUETTE:** llamado también el “Protocolo y Buenas Costumbres Virtuales”, que es un conjunto de normas morales que dentro de los usuarios de las redes informáticas, cada día se populariza más y que están haciendo de las comunidades de usuarios verdaderas sociedades digitales.

**NOM-168:** NOM-168-SSA1-1998.

**OCDE:** Organización para la Cooperación y el Desarrollo Económicos.

**ONU:** Organización de las Naciones Unidas.

**PAN:** Partido Acción Nacional.

**PIB:** Producto Interno Bruto.

**PRD:** Partido de la Revolución Democrática.

**PRI:** Partido Revolucionario Institucional.

**PROTOCOLO:** Conjunto de reglas formales que describen la forma en que se transmiten los datos entre dos o más ordenadores, pero especialmente a través de la Red.

**PT:** Partido del Trabajo.

**PVEM:** Partido Verde Ecologista de México.

**PyME:** Es el acrónimo de pequeña y mediana Empresa.

**RAM:** Del Inglés Random Acces Memory, que en términos técnicos significa Memoria de solo acceso; es un espacio de memoria volátil del ordenador que se utiliza sólo para

almacenar las operaciones que está ejecutando la computadora en el momento, esta memoria determina el número de operaciones por segundo que es capaz de realizar una computadora, por lo que entre mayor sea el tamaño del RAM, mayor será el número de operaciones que será capaz de realizar.

**SGSTI:** Sistema de Gestión de Servicios de Tecnologías de Información.

**SHCP:** Secretaria de Hacienda y Crédito Público.

**SIC:** Sociedades de Información Crediticia.

**TIC:** Tecnologías de la Información y las Comunicaciones.

**UE:** Unión Europea.

**USER FRIENDLY:** Es el nombre en inglés de un sistema de comunicación con las computadoras que hace que la interacción máquina-usuario sea simple. Hoy en día la mayoría de los programas usan esta directriz, y es lo que ha hecho tan popular a los sistemas operativos como Windows, que está basado en “ventanas” y que obtiene el máximo provecho del uso del mouse.

**WIRELESS APPLICATION PROTOCOL:** Del Inglés Protocolo de Aplicación Inalámbrica.