UNIVERSIDAD MICHOACANA DE SAN NICOLÁS DE HIDALGO
FACULTAD DE DERECHO Y CIENCIAS SOCIALES
DIVISIÓN DE ESTUDIOS DE POSGRADO

LA PROTECCIÓN DE DATOS PERSONALES POR LAS EMPRESAS MEXICANAS DEDICADAS AL E-COMMERCE EN LA UE

Tesis que para obtener el título de Maestra en Derecho de la Información

Presenta:

LIC. CAROLINA ELIZABETH FABELA GERÓNIMO

Directora de tesis:

DRA. MARÍA TERESA VIZCAÍNO LÓPEZ

Co-directora de tesis:

DRA. MARÍA ELENA PINEDA SOLORIO

MORELIA, MICHOACÁN, MAYO DE 2019

DEDICATORÍA

A mi familia,

Quienes me han apoyado en todo momento para la realización de este proyecto.

AGRADECIMIENTOS

En primeros términos agradezco infinitamente a mi universidad, la Universidad Michoacana de San Nicolás de Hidalgo, quien a través de la División de Estudios de Posgrado de la Facultad de Derecho y Ciencias Sociales ofrece esta maestría tan innovadora que tuve el gusto de cursar, la Maestría en Derecho de la Información. Ha sido un honor formarme como Maestra en Derecho en esta casa de estudios.

Agradezco a la Comisión Nacional de Ciencia y Tecnología (CONACYT), el presente trabajo de investigación fue realizado gracias al programa de becas que esta H. Institución ofrece.

A los profesores que a lo largo de la preparación del presente trabajo, tuve la fortuna y el honor de poder aprender de ellos y quienes me orientaron y apoyaron en todo momento para dar un sentido adecuado a la presente tesis. La Dra. María Teresa Vizcaíno López, quien fungió como mi directora de tesis y de quién recopilo enseñanzas valiosas, tanto académicas como personales, la perseverancia y la paciencia son puntos clave que tuve el honor de aprender de ella. La Dra. María Elena Pineda, mi co-directora de tesis, quien aportó en la orientación doctrinal de esta investigación, así como a la Dra. Monserrat Olivos Fuentes y al Dr. Carlos Rodríguez Camarena, mis profesores metodológicos de investigación, quienes me apoyaron en estructurar el presente trabajo. Agradezco a la Dra. Teresa Rodríguez de las Heras Ballell, de la Universidad Carlos III de Madrid y al Dr. Miguel Ángel Pendón Meléndez, de la Universidad de Cádiz; ambos profesores que me recibieron y ayudaron durante mi estancia de investigación en España a reflexionar la importancia del tema que ahora presento, gracias a su amplia experiencia en tema, tanto académica como profesional, contribuyeron en gran medida a la creación de la posición académica que se presenta en esta investigación.

Por último, y no menos importante, a mi familia, quienes han estado presentes desde el primer momento en que decidí comenzar esta travesía y de quienes no he recibido más que muestras de apoyo y sinceras bendiciones.

ÍNDICE

RESUMEN……...*vii*
ABSTRACT……...*vii*
SIGLAS……*viii*
INTRODUCCIÓN……..*x*

CAPÍTULO 1

LA PROTECCIÓN DE DATOS PERSONALES: DEFINICIÓN Y CONCEPTOS

1.1. El derecho a la intimidad 1
1.1.1 Teoría de los círculos 4
1.1.2 Teoría de los mosaicos 5
1.2. El derecho a la privacidad 6
1.2.1 Breve marco histórico del origen de la protección de datos personales 6
1.2.2. La protección de datos personales en México 9
1.2.3. España como país regulador de datos personales 15
1.3. El valor social y económico de la información 26

CAPÍTULO 2

LA PROTECCIÓN DE DATOS PERSONALES EN EL COMERCIO ELECTRÓNICO

2.1. El comercio electrónico y sus principios básicos 34
2.1.1. Principio de equivalencia funcional 38
2.1.2. Principio de neutralidad tecnológica 40
2.1.3. Principio de no alteración del derecho pre-existente (o Principio de subsistencia) 42
2.1.4. Principio de la no discriminación 43
2.2. Evolución histórica del comercio internacional electrónico 43
2.3. El comercio electrónico como herramienta para el proceso de transformación de la economía digital 47
2.4. La protección de datos personales en el comercio electrónico 49
2.4.1. En México 49

2.4.2. En el ámbito internacional 52

2.5. Elementos comparativos a la normativa jurídica del derecho derivados del e-commerce en México y la Unión Europea 62

CAPÍTULO 3

EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS PERSONALES DE LA UNIÓN EUROPEA

3.1. Proceso histórico de adaptación del Reglamento General de Protección de Datos de la Unión Europea 64

3.2. Análisis de principales normatividades de protección de información para el comercio electrónico 68

3.2.1. Evaluación y control de riesgos de la información 70

3.2.2. El delegado de protección de datos personales 71

3.3. Análisis de principales derechos inherentes a las tecnologías de la información en materia de protección de datos personales para el comercio electrónico contenidos en el Reglamento General de Protección de Datos 74

3.3.1. Derecho de acceso de información 78

3.3.2. Derecho de portabilidad 82

3.3.3. Libertad de información 85

3.3.4. Control de información 86

3.3.5. Derecho de supresión de datos (Derecho al olvido) 88

3.4. La regulación internacional del Reglamento General de Protección de Datos dentro de la Unión Europea, estudio comparativo 91

3.5. Ejercicio comparativo de normativas legales en materia de protección de datos para el e-commerce: RGPD y LFPDPPP 93

CAPÍTULO 4

LA PROTECCIÓN DE DATOS PERSONALES A TRAVÉS DE PRESTADORES DE SERVICIOS ENFOCADOS AL E-COMMERCE: CASO MÉXICO

4.1. El comercio electrónico en México 99

4.2. El comercio internacional electrónico en México 103

4.3. El tratamiento de datos personales por empresas transnacionales que operan en México 109

4.4. El tratamiento de datos personales por micros, pequeñas y medianas empresas 110

4.5. Los problemas de aplicación de la normativa interna para protección de datos personales a los actos realizados a través del e-commerce en México 112

4.5.1. Avances actuales en la materia 112

4.5.2. Retos actuales 114

4.5.3. Brechas y obstáculos a superar 118

4.6. Alternativas para un adecuado cumplimiento a la protección de información de carácter personal del e-commerce en México a través de las tecnologías de la Información 121

4.6.1. Auditoria web 129

4.6.2. Seguridad del sitio desde el diseño y por defecto 130

4.6.3. Corresponsables del tratamiento 135

CONCLUSIONES 138

FUENTES DE INFORMACIÓN 143

RESUMEN

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea es una legislación que revoluciona la forma en que debe de protegerse la información en esta nueva era digital. Su normativa, con alcances extraterritoriales, pone en jaque la tradicional forma en que se trataban y protegían los datos personales de las personas físicas, por lo que cualquier empresa dedicada al *e-commerce*, sin importar su nacionalidad, deberá de acatarse a las obligaciones que impone el reglamento para llevar a cabo relaciones comerciales con cualquiera de los ciudadanos que formen parte de la UE. Las empresas mexicanas dedicadas al *e-commerce* transnacional tienen la tarea de actualizarse e innovarse para estar a la altura del cumplimiento de la normativa europea, solo así podrán continuar en el plano comercial internacional con la Unión Europea.

PALABRAS CLAVE. Protección de Datos Personales, Tecnologías de la Información y Comunicaciones, Comercio electrónico, Derecho Internacional, Información.

ABSTRACT

The General Data Protection Regulation (GDPR) of the European Union is a legislation that revolutionizes the way in which information should be protected in this new digital age. Its regulations, with extraterritorial scope, put in check the traditional way in which the personal data of the natural persons were treated and protected, so that any company dedicated to e-commerce, regardless of your nationality, must abide by the obligations imposed by the regulation to carry out business relations with any of its citizens who are part of the EU. Mexican companies dedicated to transnational e-commerce have the task of updating and innovating to live up to the fulfillment of European legislation, only so they can continue at the international commercial level with the European Union.

KEYWORDS. *Protection of Personal Data, Information Technologies and Communications, E-Commerce, International Law, Information.*

SIGLAS

AEPD	Agencia Española de Protección de Datos
ANTAD	Asociación Nacional de Tiendas de Autoservicio y Departamentales
ARCO	Acceso, Rectificación, Cancelación y Oposición
CE	Comisión Europea
CCo	Código de Comercio
CNUDMI	Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
CNPD	Comissão Nacional de Protecção de Dados (Portugal)
CONCANACO	Confederación de Cámaras Nacionales de Comercio
CONDUCEF	Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros
CPEUM	Constitución Política de los Estados Unidos Mexicanos
DPO	Data Protection Officer
FCC	Federal Communication Commission
IFT	Instituto Federal de Telecomunicaciones
IMPI	Instituto Mexicano de Propiedad Industrial
INAI	Instituto Nacional de Acceso a la Información
INDAUTOR	Instituto Nacional de Derechos de Autor
LFPDPPP	Ley Federal de Protección de Datos Personales en Posesión de los Particulares
LOPD	Ley Orgánica de Protección de Datos (España)
LORTAD	Ley Orgánica de Regulación del Tratamiento Automatizado de Datos
MiPyMES	Micros, Pequeñas y Medianas Empresas
PyMEs	Pequeñas y Medianas Empresas
RGPD	Reglamento General de Protección de Datos
SE	Secretaría de Economía

TFUE	Tratado de Funcionamiento de la Unión Europea
TICs	Tecnologías de la Información y las Comunicaciones
TLCUEM	Tratado de Libre Comercio Unión Europea- México
OCDE	Organización de Cooperación y el Desarrollo Económico
ONU	Organización de las Naciones Unidas
UE	Unión Europea

INTRODUCCIÓN

El acercamiento de las TICs en la vida cotidiana de las personas, ha logrado acaparar la atención de los estudiosos del derecho mexicano, quienes han reconocido que el legislador tiene la necesidad de regular nuevos campos jurídicos que el uso de las tecnologías ha provocado, uno de ellos es el flujo transfronterizo de información de carácter personal que diariamente vive en diversos servidores a través de Internet y que, en la mayoría de las ocasiones los usuarios desconocen su ubicación de alojamiento y el tratamiento final que sin su consentimiento pueden estar dándoles los diversos prestadores de servicios a los que se les proporcionó.

En el ámbito internacional se ha elaborado y aplicado un reglamento en materia de protección de datos personales, el llamado Reglamento General de Protección de Datos (RGPD), el cual es de aplicación obligatoria para los 28 países que actualmente conforman la Unión Europea (UE) y para cualesquiera otro país que trate datos de algún ciudadano europeo que sea parte de la misma UE, lo anterior ha provocado un refuerzo en las medidas de seguridad empleadas hasta ahora para garantizar la protección de información de carácter personal que se recaba a la hora de realizar alguna transacción comercial en línea.

Asimismo, derivado de las disposiciones contenidas en el RGPD se dio a conocer que las empresas cuya principal actividad sea la del comercio electrónico dirigido a la UE, eran las encargadas de velar por la protección de la información, lo que significó una medida obligatoria para cualquier empresa que trata datos de carácter personal, independientemente de la nacionalidad con que cuente, y se convirtió en una disposición obligatoria el conocer de primera mano la normativa que se incorporó al mercado internacional para atender de manera directa las

disposiciones legales que UE impone hoy en día para realizar comercio electrónico internacional.

El RGPD estableció que toda empresa, incluyendo las empresas mexicanas que lleven a cabo operaciones de *e-commerce* en territorio europeo, deben de estar a la vanguardia en el conocimiento mínimo legal que se exige en materia de protección de datos personales en la UE, solo así podían estar en la misma posibilidad de crear conexiones mercantiles adecuadas para lograr lazos comerciales entre los demás Estados y evitar las penalizaciones y multas exorbitantes que el mismo RGPD de la UE impone.

La presente investigación nació con un objetivo, el conocer cuáles son las principales obligaciones que impone el RGPD y cuáles de ellas tienen que cumplir las empresas mexicanas dedicadas al *e-commerce* transnacional, toda vez que existen empresas mexicanas que realizan transacciones mercantiles que derivan del comercio internacional electrónico a través de operaciones de *e-commerce*; ya sea desde la venta de algún producto hacia el mercado de la Unión Europea, la oferta de servicios de vuelos u hoteles para un viaje de placer o negocios hacia los ciudadanos miembros de la UE, o la oferta de algún servicio ofrecido desde México para la propia UE, todos estos ejemplos se realiza en un marco bilateral, por lo que empresas mexicanas han comenzado a tener presencia internacional en la UE, con motivo de las llamada globalización a partir del uso de las TICs.

Durante la investigación se trató el estudio de los requisitos que solicita la UE en materia de protección de datos personales a las empresas mexicanas dedicadas al comercio electrónico trasnacional, cuándo éstos ofrecen productos y/o servicios a alguno de los ciudadanos miembros de la UE; partiendo de la premisa de que estas transferencias de información se realicen en el marco de bilateralidad conformado por México y la UE.

Los datos personales de los ciberconsumidores que se obtienen diariamente a través de múltiples operaciones electrónicas, conforman un excesivo flujo de información que al final del día alimentan enormes bases de datos que almacenan todo tipo de información personal directa o, según sea su caso, de forma indirecta, cuya explotación es a través de diversos mecanismos

informáticos de búsqueda y empresas dedicadas a otros fines; estas actividades fueron tan frecuentes en los últimos años que legislaciones como los que conforman la UE crearon a través de ordenamientos jurídicos, reglamentos que tienen como finalidad que ese tipo de actos no sucedan.

Por lo anterior, se planteó la condición en que se encuentra la protección de información en el comercio electrónico en México, el conocer la posición en se encuentra México en este tema ayudó a concluir qué tipo de medidas de protección de información las empresas mexicanas inmiscuidas en el ámbito comercial deben implementar para proteger los datos personales, tanto de nacionales como de extranjeros y cumplir adecuadamente con el RGPD, cuándo éste último lo exija.

La investigación partió del reconocimiento de la protección de datos personales como un derecho a nivel internacional, tanto la UE como México han trabajado desde la esfera de su aplicación para proteger y regular en el tema.

Un dato personal, se define en México de acuerdo con la LFPDPPP en su artículo 3º, fracción V, como “cualquier información concerniente a una persona física identificada o identificable”; por su parte, el RGPD de la UE confirma en su artículo 4.1 la definición referida, se considera como dato personal cualquier información que identifique a una persona y ésta puede ser desde un nombre, domicilio, correo electrónico, dato bancario, redes sociales e inclusive dirección IP.

Para el caso del comercio electrónico en concreto, se conoció durante la presente investigación que toda empresa u organización tiene la obligación de proteger de manera automatizada la información que recabe y que ésta tiene que ser utilizada únicamente para las finalidades que sean autorizadas previamente por el titular de la información mediante el consentimiento expreso que se señale en cada uno de sus avisos de privacidad.

Sin embargo, fue de especial interés el considerar la vertiente de la existencia de comportamientos irregulares por parte de micros, pequeñas y medianas empresas, que desconocen o no tienen el verdadero interés de contar con buenos estándares de protección tecnológica, lo que provoca un desmedido flujo de información, principalmente los de carácter personal.

De igual forma, para llegar al cumplimiento del objetivo planteado con antelación, se anticipó una posible solución para este tema, la consideración de que con la entrada en vigor del RGPD de la UE, las empresas mexicanas dedicadas al comercio electrónico que tratan datos de algún ciudadano de la UE, debían de implementar nuevos estándares de protección de información, tal es el caso de las auditorias web, la responsabilidad de los encargados del tratamiento, así como la seguridad del sitio desde el diseño y por defecto, lo anterior para no caer en el incumplimiento de dicha normatividad y mismos que podrán encontrarse a lo largo de la presente investigación.

Por lo anterior, se consideró que las empresas mexicanas debían de implementar nuevos estándares de protección de información, apoyadas en las TICs que establezcan sistemas de protección adecuados.

Para poder llegar a la comprobación de la posible solución planteada en un inicio, se establecieron una serie de objetivos específicos los cuales se trataron durante la presente investigación:

Primeramente se describió la protección de datos personales, como un derecho fundamental, dio a conocer su evolución histórica a nivel nacional e internacional, así como los problemas jurídicos creados por las tecnológicas de la información y las comunicaciones y los ordenamientos jurídicos que las regulan.

Posteriormente se describió la evolución del comercio electrónico como figura internacional, así como la protección de datos personales en el propio comercio electrónico y el impacto que ha tenido en México hasta nuestros días.

Asimismo, se describieron las disposiciones legales que emanan del RGPD de la UE en materia de comercio electrónico, las cuales en la actualidad se consideran imprescindibles para que las empresas mexicanas que ofrecen productos y/o servicios a la UE a través del *e-commerce* conozcan e implementen y se encuentren a la altura de dar un cumplimiento adecuado a los requerimientos actuales que dicta la UE para llevar a cabo transacciones mercantiles trasnacionales en línea.

Y por último, se identificó cuál es la posición de México en el *e-commerce* transnacional y cuáles son los principales retos que tienen las empresas

mexicanas dedicadas al *e-commerce* trasnacional europeo para lograr un cumplimiento adecuado del RGPD en materia de protección de datos personales.

Los puntos referidos se dieron a conocer durante el presente trabajo a través de cada uno de sus capítulos que los componen, el primer capítulo nos habla del derecho fundamental de la protección de datos personales, partiendo del derecho a la privacidad e intimidad, así como la comprensión del derecho a través de la evolución histórica que ha tenido a través de los años por parte de los organismos nacionales e internacionales que los regulan y se hace una reflexión sobre el valor de la información como parte de la economía digital, la cual en nuestros días se considera imprescindible para el desarrollo de cualquier país en desarrollo y crecimiento.

El segundo capítulo se avocó al comercio electrónico, su evolución doctrinaría e histórica contribuyó a comprender las principales necesidades que tuvo a través de los años, y la importancia que ha tenido como herramienta para el proceso de trasformación de la economía digital ayudó a conocer la relevancia de la protección de información dentro de esta práctica comercial.

El tercer capítulo recopila los principios básicos que contiene el RGPD, el derecho de acceso a la información, el derecho a la portabilidad, la libertad de información y el Derecho de supresión de datos, mejor conocido como Derecho al olvido, son solo algunos de los principios que se incorporan al reglamento de aplicación internacional, de igual forma, al conocerlos se abrió un panorama completamente nuevo para identificar los cambios que nuestra actual regulación en México necesita y comprobar los que ya se encuentran en nuestra legislación hasta este momento.

Por último, el capítulo cuarto se centra en el *e-commerce* mexicano, se dio a conocer su evolución histórica desde su incursión en el plano nacional e internacional, así la implementación de esta forma de comercio en las prácticas mercantiles actuales. Se consideró como pieza clave estudiar a las MiPyMEs, además de las grandes corporaciones, porque estas primeras forman parte del comercio mexicano actual y sobre todo se considera que son las más vulnerables a incidir en el incumplimiento del RGPD, por el desconocimiento de un reglamento

de carácter internacional sobre un tema tan diverso que los comerciantes no consideran dentro de los primeros puntos a cuidar, hablando en términos generales de la protección de datos personales de carácter personal de sus consumidores finales.

Por lo expuesto, se considera que total relevancia primero conocer cuáles son los principales problemas de aplicación de una normativa interna de protección de datos personales y para ello, se escogieron tres temas considerados como puntos clave, 1. Los avances actuales en el tema, 2. Los retos actuales y 3. Las brechas y obstáculos s superar. Una vez que se conocieron estos puntos de una forma profunda, fue que se pudo hacer el análisis de definir si las alternativas tecnológicas propuestas eran la mejor opción para llevar a cabo un adecuado tratamiento de protección de datos personales en el *e-commerce.*

La presente investigación no habría podido llevarse a cabo sin el apoyo de diversas bases jurídicas y doctrinales que han profundizado previamente en el tema de estudio. A través de la presente investigación se hizo referencia, a diversas posturas que tienen varios expertos en el tema.

Se analizaron posturas con relación al comercio electrónico o *e-commerce* de autoría de Téllez Valdés, así como de lo señalado por Villanueva. Apoyada por los autores referenciados y con la finalidad de desarrollar un trabajo de investigación de calidad jurídica, se utilizaron como apoyos doctrinarios varios marcos teóricos de referencia.

Con respecto al marco teórico de referencia internacional sirvieron como base Tratados Internacionales en materia de Comercio y Protección de datos personales, tal es el caso de los elaborados por la CNUDMI, los desarrollados por la ONU, El TLCUEM, así como el más importante para esta investigación, el Reglamento (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD).

El marco teórico de referencia legislativo nacional utilizado durante el presente trabajo fue la CPEUM, LFPDPPP, CCo, Ley Federal de Protección al Consumidor y la LFT.

Con respecto al marco teórico conceptual: Se usaron como base de encuadramiento teórico, las aportaciones de autores como Doris Oropeza con relación al avance histórico del comercio electrónico a nivel nacional e internacional; las aportaciones de Cristos Velasco San Martín en referencia con la protección de datos personales en la UE; por su parte Julio Téllez Valdés aporta en gran medida a la importancia del comercio electrónico en México, así como las aportaciones que Ernesto Villanueva hace en referencia a la importancia del Internet en la actualidad.

De igual forma, durante la elaboración de la presente investigación, se realizaron dos estancias de investigación en un país que forma parte de la UE, España fue la elegida para realizar un estudio de comparativo de la aplicación de la normativa, primeramente por la similitud y por los enlaces históricos, sociales y comerciales que mantiene con México y en segundo término, por ser un país activo dentro de los países miembros que componen a la UE. La realización de la investigación en dicho país fue conveniente, toda vez que pudo verse de cerca el impacto directo que tiene una normativa en materia de protección de datos y sobre todo porque pudo captarse esa inspiración para proteger el derecho fundamental de la protección de datos.

Por último, pero no menos importante, para llevar a cabo una correcta comprobación de la hipótesis planteada, se puede afirmar que en términos generales se realizó una investigación descriptiva utilizando los siguientes métodos:

En los capítulos primero, segundo y tercero, se utilizó el método histórico, sustentándose en la necesidad de exponer la evolución de la protección de datos personales, los avances tecnológicos en este caso, el *e-commerce* y de la regulación en torno de la misma, con la finalidad de dilucidar las oportunidades de mejora que se pudieran aplicar en las operaciones internacionales del *e-commerce.*

En los capítulos segundo y tercero se utilizó el método comparativo, que nos permitió conocer el pensamiento jurídico de otras épocas y de otros países con respecto al tema de estudio, así como los criterios que se han tomado para ubicar los diversos derechos que existen.

En los capítulos tercero y cuarto se utilizó el método analítico, en virtud de las diversas fuentes de consulta que soportaron la presente investigación, con el objetivo de sustentar el reconocimiento y necesidad de una adecuada regulación respecto a la protección de datos personales en el comercio electrónico internacional.

Por último, sirvió como base en el capítulo cuarto el método deductivo, toda vez que, en primer término se expusieron conceptos generales relacionados con la protección de datos personales, el comercio electrónico, y la aplicación del RGPD, con base a ello, se lograron identificar los aspectos concretos de su aplicación en las empresas mexicanas que llevan a cabo actividades que derivan del e-*commerce.*

La presente investigación podría llegar a parecer con un aire impositivo, es decir, estipular de manera reiterada y ferviente las nuevas disposiciones que un ordenamiento extranjero trata de imponerse a nuestra legislación por encima de la nuestra. Se solicita leer el presente trabajo con otra perspectiva, este trabajo se ha hecho con la finalidad de apoyar a las empresas que tienen relaciones comerciales con la UE a través del *e-commerce*, y para aquellas que desean comenzar relaciones con la propia UE. Si México desea crear relaciones comerciales con la UE y sobre todo mantener esa buena relación mercantil, es imprescindible que conozca de primera mano las obligaciones que dicta un nuevo cliente internacional, lo anterior, es visualizándolo desde una perspectiva de cumplimiento normativo, sin embargo, es importante comenzar a tomar como propias las intenciones que tiene el mercado europeo, que son proteger los datos personales de sus nacionales, para ofrecerles una mejor calidad de vida a largo plazo.

CAPÍTULO 1
LA PROTECCIÓN DE DATOS PERSONALES: DEFINICIÓN Y CONCEPTOS

SUMARIO: *1.1. El derecho a la intimidad; 1.2. El derecho a la privacidad; 1.3. El valor social y económico de la información.*

En el presente capítulo se podrá apreciar al derecho a la protección de datos personales, como parte de su naturaleza como derecho fundamental, los actos sociales y económicos que dieron origen a su reconocimiento, así como la evolución histórica que a través de los años, ha consolidado su reconocimiento tanto a nivel nacional como internacional.

1.1. El derecho a la intimidad

El derecho a la intimidad, es uno de los derechos considerados como fundamentales, el cual fue reconocido en primeros términos por la Declaración Universal de los Derechos Humanos promulgada en el año de 1948, mismo, dentro de su artículo 12 señala que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio, o su correspondencia, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". De lo anterior, se puede definir al derecho a la intimidad como el derecho que posee toda persona para defender la esfera más íntima de su persona, en este sentido, su información de carácter personal.

A través del reconocimiento de este derecho, varios países del mundo han buscado elementos necesarios para poder llegar a la raíz del concepto y encontrar una regulación adecuada al tema.

Como resultado de la búsqueda de dar solución a un problema social de esta naturaleza, los países pioneros en la protección de información estaban de acuerdo entre sí de una cosa en específico, el derecho a la privacidad de toda persona proviene directamente del derecho a la intimidad, y que, este derecho únicamente podía ser resguardado a través de la protección de datos personales.

Tal y como señala Rebolledo Delgado, quien afirma que "frente a la disparidad de formas, criterios y contenidos, en el reconocimiento constitucional es difícil aplicar un criterio aglutinador"[1], es decir, la forma en que varios países han llevado a cabo la regulación y la forma de proteger el derecho a la intimidad de una persona ha dependido del estilo de vida de una sociedad, el tipo de derecho al que están sujetos y las necesidades individuales que cada sociedad tiene.

Para que los Estados estuvieran en posibilidad de crear un tipo de normatividad que proteja el derecho a la intimidad de toda persona y que ésta sea utilizada como una excepción personal, se basaron en tres niveles globales de protección reconocidos internacionalmente, sin embargo, se han coincidido en ciertos temas que provocan un reconocimiento de manera global, que tiene como fin atacar las situaciones que "vulneren o intenten violar la intimidad, como lo es la informática, y de forma concreta, lo referido a la protección de datos de carácter personal"[2].

El conocer un panorama histórico de la protección de datos personales solo puede ser posible partiendo desde el punto de vista de las definiciones entre la privacidad e intimidad, avocándose a conocer sobre la evolución histórica de la protección de datos sin olvidar partir del concepto de privacidad e intimidad, a los cuales se le conoce como los pilares doctrinarios del concepto de protección de datos personales.

De acuerdo con lo señalado con la autora Garriga Domínguez "lo íntimo y lo privado se han ido desarrollando a costa de lo público"[3], no es de extrañarse que

---

[1] Rebolledo Delgado, Lucrecio, *Vida privada y protección de datos: Un acercamiento a la regulación internacional Europea y Española*, México, UNAM, p. 276.

[2] *Ibidem*, p. 277.

[3] Garriga Domínguez, Ana, *Tratamiento de datos personales y Derechos Fundamentales*, Madrid, Dykinson, 2014, p. 16.

partiendo de lo que muestra una sociedad es que se extrajo el derecho de conservar una identidad propia y el derecho de mostrarla a los demás miembros de la sociedad o a conservarla dentro de su esfera intima.

La autora Garriga Domínguez afirma lo siguiente “desde un principio la noción de intimidad se encuentra íntimamente relacionada con la posibilidad del aislamiento físico del individuo, definiéndose por primera vez el derecho a la intimidad como el derecho a estar solo o a no ser molestado”[4].

Uno de los principales textos que dieron origen al concepto de la intimidad fue a través de los autores de origen estadounidense, Samuel D. Warren y Louis D. Brandeis, quienes en su libro *Right to privacy,* sentaron las bases del reconocimiento al derecho a estar solo y denominarlo como derecho a la intimidad[5].

En la mencionada publicación, los autores partieron de la idea de encontrar una regulación jurídica adecuada que permitiera establecer limitantes para la desmedida utilización de los medios de prensa hacia los aspectos privados de la personas; con el fin de establecer una regulación adecuada es que llegaron a la conclusión de que “el derecho a la intimidad se caracteriza por cualquier rechazo a toda intromisión no consentida”[6], es decir, siempre se entenderá como una abstención de una acción.

De manera general, existen tres formas en que una sociedad se basa para poder facilitar la protección al derecho de la intimidad que garantiza a sus ciudadanos, toda vez que es prácticamente imposible que todos los ordenamientos funcionen bajo un solo y mismo estándar de protección.

Las tres formas o niveles de protección son los siguientes[7]:

- El primer nivel. Constituido por aquellos ordenamientos en que la intimidad tiene un reconocimiento pleno y explícito a nivel constitucional.

[4] *Ibidem*, p. 19.
[5] Lucas Murillo de la Cueva, Pablo, *El derecho a la autodeterminación informativa*, Madrid, Tecnos, 1990, p. 60.
[6] *Idem.*
[7] *Idem*.

- Un segundo nivel. Lo integran aquellas constituciones que acogen únicamente manifestaciones del derecho y realizan referencias genéricas o globales de acuerdo a la transferencia de datos.
- Un tercer nivel, el más bajo. El cual engloba aquellas normas supremas que no recogen ni el derecho ni sus diversas manifestaciones.

Para que los Estados se encuentren en posibilidades de crear un tipo de normatividad que proteja el derecho a la intimidad de toda persona, se han basado en estos tres niveles globales de protección, sin embargo han coincidido ciertos temas que provocan un reconocimiento de manera global, que tiene como fin atacar las situaciones que "vulneren o intenten violar la intimidad, como lo es la informática, y de forma concreta, lo referido a la protección de datos de carácter personal"[8].

De igual forma, el derecho de la intimidad se ha basado a través de la visualización y estudio de diferentes doctrinas y teorías que enfocan su estudio a un fenómeno determinado, tal es el caso de la teoría de los círculos y la teoría del mosaico.

1.1.1 Teoría de los círculos

La teoría de las esferas o de los círculos de acuerdo a lo definido por Rebolledo Delgado, señala que "el núcleo, lo más interior lo constituye lo íntimo, en una parte más externa encontramos lo familiar, en otra, lo secreto o confidencial, siendo la última esfera lo público"[9].

Otros autores como Abad, afirman que "la mejor definición de esta teoría es, la esfera de la intimidad, pero rodeándola, está la de la vida privada; y todo lo que queda fuera de ella constituye la vida pública"[10], por lo que es menester tener en

[8] *Ibidem,* p. 277.
[9] Rebolledo Delgado, Lucrecio*, op. cit.,* p. 288.
[10] Abad Alcalá, Leopoldo, "La lucha por la intimidad en internet", *La libertad de información*, Madrid, Seminario Complutense de telecomunicaciones e información, 2001, pp. 198-205, *http://pendientedemigracion.ucm.es/info/cyberlaw/actual/9/leg04-09-01.htm*

consideración las principales diferencias que pueden identificarse cuando una información pasa de ser privada a pública y las pequeñas acciones que cada uno de los individuos realiza para transferirse de una a otra[11].

Por lo anterior, esta teoría tiene como base la esfera más privada de la persona, la cual debe de observarse como algo interno que guarda el ser humano dentro de su intereses más cercanos, no debe de considerársele fuera de esos intereses personales, toda vez que esos ya son públicos y cualquier persona podría comenzar a inspeccionar en ellos, sin embargo, esta misma teoría da a entender un punto importante en la protección de la intimidad de las personas, toda vez que este un derecho que cada uno posee para acceder o restringir que las demás personas puedan acceder a su núcleo más íntimo e interfieran en él.

1.1.2 Teoría de los mosaicos

Con respecto a esta teoría, algunos autores como Abad afirman que, en la teoría del mosaico:

> Se niega cualquier vivencia aisladamente considerada valor o significado por sí misma, ya que éste sólo llegaría a alcanzarlo en combinación con otras que funcionarían de modo a como lo hacen las teselas de un mosaico, dando aquí como fruto una perspectiva de la vida privada de cada persona atendiendo a sus particulares circunstancias[12].

Ambas teorías sirven de apoyo para que, junto con la observación de determinadas necesidades que a lo largo de los años ha requerido la sociedad, se

[11] Esta teoría surge directamente de la protección de la intimidad de las personas, pero visualizando nuevos fenómenos que cada día son más comunes en la vida diaria, tal es el caso de la tecnología y de las nuevas creaciones informáticas. Tal y como lo define Madrid Conesa, "hoy, los conceptos de lo público y lo privado son relativos, pues existen datos que a priori, son irrelevantes desde el punto de vista del derecho a la intimidad, pero unidos con otros, pueden servir para configurar una idea prácticamente completa", esta teoría la define de esta forma, toda vez que como la misma autora lo señala, el derecho individual de una persona que emana desde lo más intimo, o dicho de otra forma, desde lo más personal, en sí, no conlleva mucha importancia; sin embargo, si todos esos pequeños derechos se van fusionando con otros, ya sea de esa misma persona o de un conjunto de personas, van tomando una forma determinada y fuerza para que sean dignos de observancia y protección directa del Estado frente a las demás personas.

[12] Abad Alcalá, Leopoldo, *op. cit.*

pueda comenzar a crear una ciencia jurídica que tenga como fin la protección del derecho a la intimidad de toda persona. La protección de la vida privada de toda persona se ha dado a través de los años como resultado de un método jurídico aplicado específicamente a una necesidad, por lo que es necesario que se haga el reconocimiento adecuado y se le tome la importancia para su regulación y protección.

1.2. El derecho a la privacidad

El derecho a la privacidad nació con la urgente necesidad de proteger la esfera privada de toda persona y su regulación se dio como resultado de la observación de varios fenómenos históricos y sociales que demandaron su protección jurídica; lo anterior, para poder identificar que la privacidad será en todo momento separada de lo que la sociedad conoce como público, en líneas posteriores se podrá apreciar la evolución histórica que ha tenido lugar este derecho tanto en la esfera internacional como en México.

1.2.1 Breve marco histórico del origen de la protección de datos personales

Tal y como lo ha señalado Rebolledo Delgado, “es una circunstancia constatada que las normas surgen como una consecuencia de una necesidad social, lo que hace del derecho una fórmula para solucionar conflictos”[13].Por lo anterior, se determina que uno de los principales elementos que toma el derecho para crear ciencia jurídica son las necesidades sociales que experimentan una población determinada y esto solo puede darse a través de la observación de fenómenos históricos que se han dado a medida del transcurso de los años.

Así, se considera necesario el estudio de las necesidades históricas que dieron origen a la búsqueda generalizada de los Estados de proteger el derecho a intimidad de las personas, a través de la protección de datos de carácter personal.

[13] Rebolledo Delgado, Lucrecio, *op. cit.,* p. 292.

Claro está que el fenómeno de la protección de datos personales se ha visualizado y tomado en cuenta con más antelación de lo que comenzó a regularse en el tema.

De igual forma, es importante señalar que los países pioneros en la protección de datos personales han sido aquellos que han experimentado una oleada de vulneraciones sociales a través de la irrupción y uso indebido de datos personales. “Alemania ha sido uno de los precursores del derecho a la autodeterminación informativa para cada individuo, porque sabe del riesgo que implica acumular información sobre las personas para ejercer control sobre sus destinos”[14].

Al término de la segunda guerra mundial, al realizar toda la búsqueda de factores que llevaron a cabo la realización del holocausto, el cual consistió en la matanza de más de 6 millones de judíos, se realizaron el siguiente cuestionamiento. ¿Cómo había sido posible la captura tan minuciosa de tanta gente?, Posteriormente se conoció que existían listas en las cuales se especificaban los orígenes, antecedentes, ideólogas y características específicas de las personas que comprendían el grupo de personas que conformaban la raza judía. “El gobierno alemán comenzó a recopilar los catálogos de tarjetas de identificación de enemigos políticos y raciales del Reich alemán y así lograron su cometido, el del prácticamente exterminio de la clase judía”[15].

Una vez concluida la segunda guerra mundial, como resultado de una búsqueda de todos los países del mundo para encontrar paz entre ellos, se unieron para realizar pactos de fraternidad y proteger los derechos humanos de toda persona, fue así como se llevó a cabo la firma de la Declaración Universal de los Derecho Humanos de las Naciones Unidas, quienes entre otras cosas defendían la privacidad de toda persona, como una forma de proteger los derechos y reconociéndolos como derechos fundamentales. A partir de ese

[14] Cerda Silva, Alberto, “El nivel adecuado de protección, para las transferencias internacionales de datos personales desde la Unión Europea”, *Revista de Derecho Valparaíso*, núm. 36, p. 327.
[15] Tornabene, Inés, “Protección de Datos Personales: repasando un poco de Historia, del Tercer Reich a Facebook”, *Revista CSO business advisor*, 26 de febrero de 2015, *http://www.cxo2cso.com/2015/02/proteccion-de-datos-personales.html.*

momento se comenzó a resguardar de manera reiterada la información que componía la vida privada de una persona, sin embargo, no se reconocía completamente su importancia en el tema.

En virtud de lo anterior, se reflexiona de que este punto de partida fue clave para visualizar la necesidad de proteger los datos personales de las personas, aunque no alcanzaban a apreciar todos los campos en que la información podría participar, una cosa si tenían claro, sabían la responsabilidad y el riesgo que era, que toda esa información se encontrará en las manos equivocadas.

Años más tarde, con la aparición de las TICs, comenzó a visualizarse la problemática que su uso podría traer para la protección de los datos personales, tanto a nivel nacional como internacional; ya que en esa ocasión, los países consideraban que quizás existiría protección en su esfera de comunicación que les brinda su país, pero tal y como lo señala Cerda Silva "la ausencia de leyes en otros países y la precaria armonización legal entre otros impedían la obtención de tal logro"[16].

Tal y como lo señala Garriga Domínguez, "La revolución tecnológica del Siglo XX condujo a lo que se denominó civilización cibernética, que significó el inicio de una nueva era que planteó nuevos retos éticos"[17],por lo que, la civilización cibernética creó importantes cambios dentro del estilo de vida de las personas de todo el mundo, desde el punto de vista cultural y social; nuestra forma de comunicación y de interacción cambió, por lo que no se encontró en sentido descabellado el que una nueva forma de regir esas relaciones, tenía que comenzar a regularse.

Como consecuencia de tal razonamiento, los países comenzaron a visualizar la necesidad de realizar nueva reglamentación para empezar a crear lazos de participación entre los diferentes países, a principios de la época de 1980, "resultaba evidente que dichos países necesitaban una aproximación

[16] Cerda Silva, Alberto*, op. cit*., p. 327.

[17] Garriga Domínguez, Ana, *Tratamiento de datos personales y Derechos fundamentales: Desde Hollerith hasta Internet*, México, HuriEge, Consolider ingenio, 2010, p. 8.

internacional para lograr cierta concordancia entre sus legislaciones locales y, en especial, regular las transferencias de información personal de un país a otro"[18].

Lo anterior arroja como conclusión que la protección de información es un tema en el que los países hoy en día han reconocido su importancia y apuestan por su protección, los cuales, han comenzado a cuestionarse las consecuencias que las practicas desleales de tratamiento traerían consigo, por lo que, han trabajado en su protección que va más allá de su ámbito territorial.

1.2.2. La protección de datos personales en México

Al igual que en otros países del mundo, México ha trabajado desde su esfera legal de aplicación en la protección de datos personales, ha reconocido a través de su máximo ordenamiento legal la CPEUM, también conocida como Carta Magna, así como en diversos ordenamientos que ha creado, confeccionado y perfeccionado, la definición y aplicación de este precepto, derivado del derecho a la privacidad, el conocer su ubicación y respaldo legal que le ha dado en derecho en México, ayudará a comprender la importancia de su conocimiento y el ejercicio general a favor de la sociedad.

1.2.2.1. Origen y evolución

Uno de los derechos humanos reconocido por la CPEUM, es el derecho a la privacidad; el cual se consagra en el artículo 16 de la CPEUM, mismo que a la letra señala "las comunicaciones privadas son inviolables: la ley sancionara penalmente cualquier acto que atente contra la libertad y privacía de las mismas".

Esta es una de las razones por la que las comunicaciones hoy en día deben de tener un cuidado especial para su divulgación, así como la protección en todo momento a la privacidad de las personas que emiten esa información, ninguna persona puede ser vulnerada en cuanto a conocer la información que emita, a

[18] Cerda Silva, Alberto*, op. cit*.

menos que se trate por motivo de un delito y que previamente se levante una solicitud por alguna autoridad competente para llevar a cabo dichas situaciones.

La importancia de la privacidad ha sido estudiada y discutida por una esfera importante de comunidad empresarial, académica y social, quienes piden que se realicen unas políticas específicas para la protección de este derecho en el ámbito de aplicación de la esfera digital.

Inclusive se ha llegado a analizar la relación que existe entre la propia privacidad con la protección de datos y la innovación y al respecto se ha señalado por autores como Miguel Recio, lo siguiente:

> La tensión que existe entre protección de datos personales o privacidad e innovación es necesaria, ya que la innovación permite plantear cuestiones que hacen que el derecho a la protección de datos o privacidad evolucione, mientras que la protección de datos personales o privacidad aplicada a la innovación permite generar la confianza necesaria. Por tanto, se trata de una relación mutua y que implica que la protección de datos personales y la innovación, sean compatibles[19].

Es importante recalcar que el autor asimismo señala que la sinergia de estos tres elementos que generaron la necesidad de protección de los datos personales han provocado que se tengan que crear medidas para salvaguardar este tipo de innovaciones, tal y como afirma el autor:

> más que nunca, dado el álgido en el que nos encontramos en cuanto a la innovación tecnológica y los modelos de negocios, así como a la necesidad de garantizar el derecho fundamental a la protección de datos personales, es necesario encontrar un equilibrio que se plasme en una norma internacional, vinculante y adaptable[20]

Por motivo de lo anterior, en el año 2008 entonces Instituto de Federal de Acceso a la Información Pública, bajo una investigación se centró en dar a conocer la posición en la que se encontraba México con respecto a la protección de datos personales. En el mismo se señalan algunos de los avances históricos que provocaron la urgente necesidad de contar con una ley de protección de datos

[19] Recio Gayo, Miguel, *Protección de Datos Personales e Innovación ¿(in)compatibles?,* Madrid, Reus, Colección de Derechos de la Nuevas Tecnologías, 2016, p. 7
[20] *Ibidem,* p. 9

personales para la sociedad actual, y sobre todo para la sociedad mexicana, frente a todos los demás países del mundo.

Se ha afirmado por el Instituto que el uso de las tecnologías es una de las principales causas que han dado origen a la necesidad de contar con la protección de datos personales, toda vez que se afirma, "Ya no es posible concebir la vida de los seres humanos ni su interacción, sin el uso de tecnologías informáticas *urbi et orbi*. Dicha expansión conlleva el intercambio de flujos de información de todo tipo, incluida la relativa a las personas"[21]

Así mismo, se ha llegado a afirmar que "el hecho de que los avances tecnológicos permitan irrumpir silenciosamente en el ámbito de lo privado, vulnera la esfera de uno de los derechos fundamentales de los individuos, el de la privacidad"[22].

El ciberespacio se ha convertido en un blanco elemental para contribuir con el acceso desmedido de información de las personas, que en la mayoría de los casos, desconoce completamente el paradero final de almacenamiento y tratamiento que se les da a los mismos, no es de extrañarse, que las personas no se percatan de la importancia que tiene el proporcionar sus datos personales y el alcance que tiene depositarlos en manos de entidades tanto públicas como privadas, sin antes cuestionarse con qué finalidad son recabados y cómo son tratados, "entre éstos destacan la minería de datos o la geo-localización, la detección remota o la video vigilancia, dispositivos que hoy en día han madurado y están fácilmente disponibles en cualquier lugar del mundo"[23]

La identificación de todos estos temas, originados principalmente de la red, provocó que comenzara a considerarse a la protección de datos como una prioridad, y que los países empezarán a detectar la importancia de su regulación, se llegó a la conclusión de que la protección de las personas, más allá de únicamente los datos, ha hecho que se tome en cuenta desde el punto de vista

[21] Instituto Federal de Acceso a la Información pública, *La protección de datos personales en México: una propuesta para deliberar,* julio 2018, *http://iaipoaxaca.org.mx/biblioteca_virtual/datos_personales/5.pdf*
[22] *Idem*
[23] *Idem*

jurídico. “La tecnología no puede permanecer ajena al Derecho, ni evidentemente a la Constitución, por más que la velocidad con la que ocurren las innovaciones tecnológicas amenace con hacer obsoleto cualquier esfuerzo por regular su impacto sobre el derecho a la vida privada”[24]

Posteriormente, se creó en México, la LFPDPPP, publicada en el Diario Oficial de la Federación el 27 de abril de 2010; misma que entró en vigor el día 6 de julio del mismo año. Dicho ordenamiento cuenta con 69 artículos y ocho transitorios; el mismo que tiene como finalidad de acuerdo a su artículo 1º “la protección de datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas”

Con respecto a los sujetos obligados en dicho ordenamiento y que podrán tener participación en la dicha normativa, enuncian a toda aquella persona física o moral de carácter privado que lleve dentro de sus finalidades el tratamiento de datos personales, esto puede observarse claramente en su artículo 2 de la Ley citada, asimismo en dicho artículo se puede observar claramente los casos considerados como de excepción, en los cuales esa ley no tendrá ningún tipo de responsabilidad, en tal caso se puede citar a:

- Las sociedades de información crediticia.
- Todas aquellas personas que llevan a cabo la recolección y almacenamiento de datos personales y que tenga como finalidad el uso personal, sin fines de divulgación y sin ningún fin de carácter personal.

De igual forma, se da al conocer en la ley, la definición para cada uno de los términos utilizados de manera consecutiva durante el contenido del cuerpo de dicha ley, tal es el caso del significado de lo que se refiere a un aviso de privacidad, bases de datos, responsable, consentimiento, encargados, instituto, responsable, titular, y todos aquellos términos que ayudan a una clara interpretación de la ley.

[24] *Idem*

La LFPDPPP de acuerdo con su artículo 4º enuncia como los principales principios que la rigen a “la protección de la seguridad nacional, el orden, la seguridad, la salud pública y los derechos de terceros”. Estos principios vienen respaldados desde acuerdos de carácter internacional, se trabajó en todo momento para cumplir con los estándares que la comunidad internacional exigía al estado Mexicano para garantizar los derechos de privacidad y de autodeterminación informativa de todos sus ciudadanos, consagrados desde la Declaración Universal de los Derechos Humanos de 1948.

Actualmente, la LFPDPPP cuenta con XI capítulos entre los que figuran los principios, los derechos de los titulares de los datos personales, el ejercicio de los derechos ARCO, la transferencia de los datos, las facultades del Instituto, las autoridades reguladores, el procedimiento de protección de los derechos, los procedimientos para hacer valer esos derechos, así como las infracciones y sanciones que puede imponer la autoridad encargada de regular los derechos de los ciudadanos.

Una vez creada la LFPDPPP, se creó el INAI, el cual genera anualmente un foro en el que varios sectores de la sociedad participan exponiendo los principales problemas que experimentan por la falta de regulación en la materia con respecto a los medios electrónicos y el uso del Internet, y que provoca, que no sean explotados al máximo los beneficios que el Internet proporciona a las personas y empresas para crear lazos comerciales y de comunicación.

Sin embargo, algunos autores como Velasco San Martín exponen su principal preocupación de no tener una fuente normativa en México que resguarde el derecho de protección de los datos personales de toda persona que hiciera uso de medios tecnológicos como lo es el Internet, toda vez que afirman ese derecho debería de estar respaldado por leyes justas que se preocupen por resguardar los datos personales de toda persona, ya que no debe considerarse como una necesidad banal, sino que es importante cuidar toda la información de carácter personal que circula diariamente en Internet.

El autor Velasco San Martín fundamenta su opinión de acuerdo a una comparativa de carácter internacional, entre La UE y México; de acuerdo a esta

comparativa hace gran énfasis en señalar que la mayoría de los habitantes de la UE, sí muestran su principal interés el proteger su información personal a través de la protección de sus datos personales, refiriéndose al respecto que "el 70 por ciento están preocupados de que sus datos sean mal utilizados"[25],caso contrario en México, quienes apenas comienzan a informarse acerca de las protección de este derecho, pero aún hay un desconocimiento sobre cómo protegerlo directamente o qué hacer en caso de que se vea vulnerado.

1.2.2.2. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Todas las reflexiones referidas con antelación han construido un criterio relativo a la importancia de la protección de datos personales, en México se llevó a cabo la elaboración de la LFPDPPP la cual fue publicada en el Diario Oficial de la Federación en 2010. Dicho ordenamiento cuenta con 69 artículos y ocho transitorios, mismos que tienen como finalidad de acuerdo a su artículo 1º "… de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas". Asimismo se han hecho importantes reformas a la CPEUM que nos rige, señalando en dicha información que, "en 2007, el Congreso de la Unión aprobó una reforma al artículo 6º constitucional en el que se establece la protección a los datos personales y la información relativa a la vida privada, así como el derecho de acceder y corregir sus datos que obren en archivos públicos"[26].

Una vez creada la LFPDPPP, se creó el INAI, el cual genera anualmente un foro en el que varios sectores de la sociedad participan exponiendo los principales problemas que experimentan en temas de privacidad y protección de información, por la falta de regulación en la materia con respecto a los medios electrónicos y el uso del Internet, y que provoca, que no sean explotados al máximo los beneficios

[25] Velasco San Martín, Cristos, "Privacidad y protección de datos personales en internet. ¿Es necesario contar con una regulación específica en México?", *Boletín de Política Informática,* México, núm. 1, 2003.

[26] Instituto Nacional de Acceso a la información (INAI), *Cómo ejercer tu derecho a la protección de datos personales, http://inicio.ifai.org.mx/SitePages/Como-ejercer-tu-derecho-a-proteccion-de-datos.aspx?a=m1.*

que el Internet proporciona a las personas y empresas para crear lazos comerciales y de comunicación. Sin embargo, algunos autores exponen su principal preocupación de no tener una fuente normativa en México que resguarde el derecho de protección de los datos personales de toda persona que hiciera uso de medios tecnológicos como lo son las formas de comunicación a través de Internet, toda vez que señalan que ese derecho debe de estar respaldado por leyes justas que se preocupen por resguardar los datos personales de toda persona, ya que no debe considerarse como una necesidad banal, debe de tratarse con la importancia que merece[27].

1.2.3. España como país regulador de datos personales

Europa ha sido la pionera en la protección de información de carácter personal, desde su reconocimiento a la carta de Derechos Humanos de la ONU de 1948, ha dado a través del Derecho, la protección jurídica que los Estados necesitaban para prestarle atención e importancia a su artículo, partiendo de su esencia legal y humana y de los objetivos de protección de la intimidad y que va extensivo hasta la propia imagen, confidencialidad y secreto de comunicaciones.

A pesar de lo contenido en la Carta de Derechos Humanos de la ONU mencionada con antelación, el Consejo de Europa dio reconocimiento a este derecho a partir de finales de 1960 y, a partir de ahí, varios países que conformaban parte del circulo europeo comenzaron a trabajar en la incorporación de protección de ese derecho considerándolo como fundamental. Algunos de los casos de mayor relevancia fueron las reformas elaboradas por el Consejo Consultivo del Consejo de Europa que en el año de 1967 realizó estudios de temas relacionados con la intimidad de las personas a través de los avances de las tecnologías de la información[28]; inclusive, otros textos que se realizaron a través de organismos independientes, tal fue el caso del Consejo de Europa, quien trabajó en temas de protección de información; tal y como lo comenta la autora

[27] Velasco San Martín, Cristos, *op. cit.*

[28] Ojeda Bello, Zahira, "El derecho a la protección de datos personales desde un análisis histórico-doctrinal" *Tla-melaua*, Puebla, 2015, vol. 9, núm. 38, p. 58.

Ojeda Bello “A través del Convenio 108 del Consejo de Europa, en 1981, se establecen los principios y derechos que cualquier legislación estatal debía recoger a la hora de proteger los datos de carácter personal. Hasta este momento, la perspectiva era solucionar los problemas que se suscitaban entre el uso de la informática y la intimidad de los sujetos”[29]

Tan solo es necesario comenzar a visualizar parte de estos trabajos con la interpretación de la sentencia emitida el 15 de diciembre de 1983[30], en la cual el Tribunal Federal Alemán, inclusive en contra de lo previsto por el Tribunal Europeo y de su propia Ley Hesse de 1970, emitió por primera vez el reconocimiento de la autodeterminación informativa[31]. A partir de ahí, el Tribunal Constitucional Federal Alemán, con tal decisión, le atribuye a las personas la capacidad autónoma de decisión para elegir la información personal que desea compartir y cómo compartirla; a su vez, se da lugar a la protección de esa información personal y el derecho de sus titulares para acceder a ella en el momento en que lo decida y de la forma en la que considere pertinente, autorizando o negando cualquier tipo de utilización o tratamiento[32]. Con esta resolución se dio paso al conocimiento y reconocimiento directo de derechos ahora considerados como fundamentales de la personalidad, como es el de la libre decisión de datos de carácter personal, así como la libertad para que una persona pudiera utilizarlos, transferirlos, modificarlos u oponerse a que determinada persona los utilizará sin su consentimiento, el cual resultó ser un gran paso para que el Derecho en materia de privacidad; con lo anterior, se puede considerar que a través de los años, se ha producido un avance significativa en temas de la intimidad de las personas, hasta lo que ahora se conoce como protección de datos personales, en este sentido autores como Ojeda Bello, señalan que el transcurso del tiempo solo ha

[29] *Idem.*

[30] Sentencia emitida por el Tribunal de Justicia Alemán para revisar si se protegían los datos en el censo de población de emitido el gobierno en el año de 1983.

[31] Se le llama autodeterminación informativa, de acuerdo con la misma decisión emitida por el Tribunal Constitucional Federal Alemán como el derecho que se le concede al individuo para decidir de manera libre sobre las acciones que va a realizar o que no, o según sea su caso, a omitir, incluyendo la posibilidad de obrar de hecho en forma subsecuente con la decisión adoptada.

[32] Martínez Martínez, Ricard, “El derecho fundamental a la protección de datos: perspectivas” *Revista de internet, Derecho y Política*, septiembre 2007, p. 48.

provocado que se conciba “progresiva el concepto restringido del derecho a la intimidad, que, aplicado a los avances tecnológicos, da paso a la denominación del derecho a la autodeterminación informativa o libertad informática. Años más tarde, emerge, con independencia y autonomía, un nuevo derecho fundamental, denominado derecho a la protección de datos personales”[33].

Por su parte, la Protección de Datos Personales ha estado protegida por España, desde inicios de su reconocimiento por parte de la Comisión Europea y de los Estados soberanos que la conforman, el derecho a sido protegido por el Estado español a través de la propia Constitución Española, quien en su artículo 18.4 hace reconocimiento oficial del derecho antes mencionado, señalándolo como a continuación de enuncia:

> 18.4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

De acuerdo con el propio gobierno español “Se hacía así eco de los trabajos desarrollados desde finales de la década de 1960 en el Consejo de Europa y de las pocas disposiciones legales adoptadas en países de nuestro entorno”[34]

La incorporación del derecho de la Protección de Datos en la Constitución Española se realizó por la necesidad de reconocimiento y aplicación absoluta del derecho para la protección de las personas con respecto al uso y control de sus datos, basta revisar algunas de las sentencias que a través de los años se dieron por el Tribunal Español en la materia para reafirmar la anterior aseveración, tal es el caso de la sentencia 94/1998 del 04 de mayo[35], en la que se determina el

---

[33] Ojeda Bello, Zahira, *op. cit.,* p. 59.

[34] Proyecto de Ley Orgánica De Protección De Datos Personales y Garantía De Los Derechos Digitales (Antes denominado proyecto de ley orgánica de protección de datos de carácter personal, Congreso de los Diputados, 17 de octubre de 2018, Serie A, Núm. 13-4.

[35] Sentencia 94/1998 del 04 de mayo, Se dio vista por medio del recurso de amparo 840/95 en la cual se hace revisión a una sentencia emitida por la Sentencia de la Sala de lo Social del Tribunal Superior de Justicia de Madrid, de fecha 31 de enero de 1995, dictada en procedimiento de tutela de derechos fundamentales, por el mal uso de información recabada por la empresa Renfe con respecto a uno de sus empleados para el descuento de nómina. En dicha sentencia, se concluyó que se lesionan los derechos de protección de datos del empleado frente al uso de la tecnología informática, por lo que se vulnera el ámbito más estricto de intimidad y señala que es importante

derecho de toda persona para que pueda controlar su información y para que así, se evitara el uso indebido y no autorizado de los datos de una persona sin su debido consentimiento, así como que se controlara el uso automatizado de datos, para que éstos no fueran utilizados para un fin distinto para los que fueron proporcionados.

Así mismo, la sentencia 292/2000 de 30 de noviembre[36] contribuye al derecho de protección de datos personales, toda vez que reconoce a este derecho como autónomo y regula su transferencia y uso, autorizando al titular de los datos para que éste tenga la libertad de autorizar o negar la transferencia de sus datos a un tercero y a su vez el derecho de conocer para que se están tratando y así poder decidir si continúa autorizando su tratamiento o se niega al mismo.

De manera interna, a través de los años España trabajó en la incorporación del derecho de protección de datos personales a sus legislaciones internas, creando así en el año de 1992 la Ley Orgánica para la Protección de las Personas Físicas en Relación con el Tratamiento de Datos Personales, ésta fue conocida como Ley Orgánica 5/1992, de 29 de octubre[37]. Años posteriores, la Ley 5/1992 fue reemplazada por la Ley 15/1999, de 05 de diciembre, la nueva Ley contaba con una mejor compresión de las necesidades españolas en temas de protección de datos, se introdujo en dicha ley disposiciones adicionales contempladas en el

---

controlar que la automatización de datos provoque comportamientos discriminatorios, para que estas prácticas no se lleven a cabo.

[36] Sentencia 292/2000 de 30 de noviembre, la cual da vista a conocer el acto de inconstitucionalidad contra los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal por no respetar el contenido esencial del derecho fundamental al honor y a la intimidad personal y familiar así como del derecho fundamental que este Tribunal ha denominado de "libertad informática" y que los datos que se recogen por parte de una administración pública, en ningún momento deben de comunicarse a otra u otras administraciones públicas, sea cual fueren los motivos de este acto, sin que antes se les comunique a los titulares para que puedan ejercer su derechos de autodeterminación informativa. En la misma sentencia se reconoce que los artículos 21 apartado 1 y el 24 apartado 1 y 2 de la Ley orgánica 15/1999, si son contrarias a la Constitución por lesivas del art. 18.4 de la Constitución Española, por lo que, se decide declararlas nulas de toda interpretación y aplicación.

[37] La Ley orgánica 15/1992 fue enfocada directamente al tratamiento automatizado de datos personales y fue conocida como LORTAD.

artículo 8º de la Carta de Derechos Fundamentales de la UE[38], con lo establecido en el artículo 16.1 del Tratado de funcionamiento de la UE[39] y también contaba con nuevas adaptaciones que la directiva 95/46/CE que acababa de implementarse para la UE en materia de protección de datos personales, exigía, y además de lo anterior, ya que se había estado preparando en base de todas las cuestiones jurisprudenciales que en los siguientes años se habían estado presentando en la materia, dando un enfoque especializado en cuanto al derecho de protección de datos se refería.

Años más tarde, debido a la gestión de la propia UE, de la que España es miembro activo, se comenzó a trabajar con una propuesta de ley armonizadora desde el punto de vista legal en materia de protección de datos, con ella se pretendía llegar a crear un derecho uniforme que tuviera aplicación absoluta en todos los países miembros de la Unión, para crear un marco de protección que atendiera a las necesidades de la ahora llamada globalización. Desde el año 2010 se lanzó una comisión encargada de regular los principales problemas que se estaban presentando en materia de protección de información y datos personales, enfocada principalmente a los servicios proporcionados a través de medios de la Sociedad de la Información.

Como resultado de esa comisión encargada se llegó a la creación y adaptación del Reglamento de la UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016[40], relativo a la protección de las personas físicas

[38] 2000/C 364/01 Carta de derechos establecida por los Estados miembros de la Unión Europea, con la finalidad de contribuir, preservar y fomentar los valores mínimos comunes que deberán de observar para fomentar la diversidad de culturas y tradiciones de los pueblos de Europa. El artículo 8º habla específicamente del derecho a la protección de datos de carácter personal respetando su tratamiento y el consentimiento de sus titulares, así como la facultad de una autoridad independiente para decidir sobre los asuntos que se traten en la materia.

[39] Tratado cuya principal finalidad fue establecer bases sólidas dentro los países miembros de la Unión Europea para impulsar el progreso económico y social de los Estados miembros. El artículo 16.1 está enfocado al reconocimiento del derecho de protección de datos personales con que toda persona cuenta.

[40] Este reglamento, de aplicación directa para todos los miembros que pertenezcan a la Unión Europea (UE), y o a cualesquier otro Estado que dé un tratamiento de manera directa o indirecta a algún ciudadano miembro de cualquiera de los Países miembros de la propia UE, tiene por objeto dentro de su artículo 1 “establecer las normas relativas a la protección de las personas físicas en lo

en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), así como de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo[41].

De acuerdo a lo considerado por los expertos, el actual Reglamento de la UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 "pretende con su eficacia directa superar los obstáculos que impidieron la finalidad armonizadora de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos"[42]. Para ellos, la directiva no logró concretar la finalidad armonizadora que se pretendía crear entre todos los Estados miembros de la UE, toda vez que, durante la vigencia de la Directiva 95/46/CE, cada uno de los países miembros únicamente adoptó el texto normativo de acuerdo a sus propias necesidades en materia de protección de datos, toda vez que les era más conveniente para su propia aplicación normativa; así mismo, la Directiva 95/46/CE "no ha impedido que la protección de los datos en el territorio de la Unión se aplique de manera fragmentada"[43]. De igual forma, se reconoce el papel y posición que está tomando la tecnología hoy en día y que fue motivo indispensable para que la UE "se

---

que respecta el tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos".

[41] Proyecto de Ley Orgánica de Protección De Datos Personales y Garantía de los Derechos Digitales (Antes denominado proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, Congreso de los Diputados, 17 de octubre de 2018, serie A, núms. 13-4, pp. 6-7.

[42] Proyecto de Ley Orgánica De Protección De Datos Personales y Garantía De Los Derechos Digitales (Antes denominado proyecto de ley orgánica de protección de datos de carácter personal), Congreso de los Diputados, 17 de octubre de 2018, serie A, núm. 13-4, p. 7.

[43] Considerando 9º del Reglamento de la Unión Europea (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

plateara nuevos retos en materia de protección de los datos personales, ya que la magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa"[44]

Otras de las cosas que el Reglamento de la UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 tuvo como principales objetivos, fue el regular el aumento transfronterizo de datos en el nuevo mercado interior e incluir algunos de los nuevos retos que se habían estado presentando por la inclusión de las tecnologías de la información, así como la situación globalizadora en la que sus países miembro estaban adentrándose; dentro de los considerandos del propio Reglamento de la UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, reconocen el papel de la tecnología dentro del marco de los Estados, toda vez, que ha transformado tanto la economía como vida social[45].

Con su aprobación y entrada en vigor el 25 de mayo de 2016, se comenzaron con una serie de reformas en todos los países miembros de la UE, para estar en completa armonización con lo contenido en el Reglamento de la UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, el cual otorgó un periodo de dos años para que todos los Estados miembros estuvieran a la altura de la normativa para su debido cumplimiento, por lo que se decretó que tendría aplicación obligatoria a partir del 25 de mayo de 2018. Lo anterior dio la posibilidad a los Estados de regular a través de su derecho interno normas que permitan dar cumplimiento al Reglamento y con la obligación de los propios Estados de que se incorporen medidas directamente contenidas en el Reglamento, incluso intervenir en la creación de normas adicionales no

[44] Considerando 5º del Reglamento de la Unión Europea (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

[45] De acuerdo con el considerando 6º del Reglamento de la Unión Europea (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, la tecnología también ha facilitado la libre circulación de datos personales dentro de la unión, a terceros países y a organizaciones internacionales, por lo que es necesario contar un nivel de protección de los datos personales.

contempladas en el reglamento, pero que actúen en sentido positivo a favor de los ciudadanos de su país miembro de la UE[46].

Por motivo de lo anterior, fue que España trabajó en importantes modificaciones a su última Ley 15/1999 atendiendo al principio de seguridad jurídica[47]. Debido a la gran cantidad de cambios que se establecían en el Reglamento, se tomó la decisión de "la elaboración de una nueva Ley que sustituya a la actual"[48], por lo anterior, se dio a la tarea de crear la Ley Orgánica De Protección De Datos Personales Y Garantía De Los Derechos Digitales, que sustituyó de manera plena a la actual Ley 15/1999. Esta normativa se publicó el 10 de octubre de 2018 y a partir de noviembre del mismo año ésta pasó a ser el principal ordenamiento en materia de protección de datos de carácter personal para España.

La nueva Ley Orgánica de Protección de Datos de España está conformada por noventa y siete artículos estructurados en diez títulos, veintidós disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y dieciséis disposiciones finales. Todo lo concerniente al tratamiento de datos personales se hará con resultado de la aplicación del artículo 18.4 de la Constitución Española así como a lo contenido en el Reglamento de la UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

De manera previa durante el tiempo que tardó en aprobarse la nueva Ley, España contó con el denominado Real Decreto de 5/2018 del 27 de julio, de

---

[46] De acuerdo con el considerando 10º del Reglamento de la Unión Europea (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, el Reglamento no excluye el derecho de los Estados miembros, por lo que reconoce un marco de maniobras para que los Estados miembros especifiquen sus normas, inclusive para el tratamiento de categorías especiales de datos personales.

[47] Dicho principio establece que los Estados miembros de la Unión Europea tendrán que adaptar los ordenamientos europeos en los que formen parte a sus propios ordenamientos internos de una forma clara y que sea difundido como público para que pueda accederse al conocimiento de sus ciudadanos de manera general. Es por lo anterior que, una vez establecida una normativa de esta naturaleza, lo países miembros deberán de eliminar las normas que en todo sentido sean incompatibles con el derecho Europeo, o por el contrario, serán consideradas en todo momento como invalidas.

[48] Proyecto de Ley Orgánica de Protección de Datos Personales y Garantía De Los Derechos Digitales (Antes denominado proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, Congreso de los Diputados, 17 de octubre de 2018, serie A, núms. 13-14, p. 8.

medidas urgentes para la adaptación del Derecho español a la normativa de la UE en materia de protección de datos, en el que de primer momento se integraron las disposiciones más importantes del Reglamento que debían ser observadas por España con carácter de urgente, para no caer en incumplimiento directo del Reglamento frente a la UE.

De acuerdo con el texto emitido por la Jefatura del Estado Español, a través del Boletín Oficial del Estado con fecha 30 de julio de 2018, el Real Decreto 5/2018 del 27 de julio tuvo como objeto adecuar a la legislación interna española el Reglamento de la UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en los aspectos que no admitían demora de implementación y adaptación de aquellos preceptos que no estaban contemplados en las legislaciones internas y que de manera inmediata tenían que estar siendo cumplidas por todos los miembros de la UE.

Algunas de los temas que se identificaron de manera rápida y necesaria para comenzar a implementar y observar de manera general el Reglamento, fueron los siguientes puntos[49]:

1. Identificar y designar al personal que tenía que comenzar a cumplir de manera directa y profesional con las obligaciones de investigación enfocadas a la aplicación de lo dispuesto en el artículo 58.1 del Reglamento, en el cual, se faculta para que cada una de las autoridades de control puedan designar de manera autónoma al personal encargado de llevar a cabo la tarea de implementación del Reglamento de la UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Así como determinar en qué casos iba a corresponder un régimen aplicable distinto cuándo existieran autoridades de supervisión de otros Estados miembros.
2. El reemplazo y adecuación de las sanciones que ahora se establecen en el Reglamento de la UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, toda vez que se consideró necesaria la clara delimitación de cuáles serían concretamente los sujetos que incurrirían en

[49] Real Decreto-Ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos, Boletín oficial del Estado, 30 de julio de 2018, núm. 183, p. 76250.

la responsabilidad derivada[50], y por otro lado, fijar los plazos en lo que de manera interna comenzarían a ser efectivos los plazos de prescripción de las infracciones y sanciones del propio Reglamento.

3. La regulación de los distintos procedimientos que se habían incorporado al Reglamento para los casos en que se diera lugar una vulneración de información, puntualizando tres situaciones en concreto: a) Los tratamientos transfronterizos (definidos en el artículo 4.23 del Reglamento). b) Los transfronterizos con relevancia local en algún Estado miembro (artículo 56 del Reglamento) y c) El tratamiento datos exclusivamente nacionales (artículo 55 del Reglamento)[51]. La AEPD es la que llevará a cabo el control de la información y actuará frente la UE como representante de España, por lo que actuará como autoridad de control.

1.2.3.1. La Agencia Española de Protección de Datos Personales

La elaboración de la Ley 15/1999 dio como resultado de su propia normatividad la creación de una agencia de protección de datos, toda vez que de acuerdo a la Ley 15/1999 artículo 35 fracción primera a la letra señala: “La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena

[50] Al referirse de responsabilidades derivadas hay que considerarse las diferentes responsabilidades derivadas del tratamiento y explotación de los datos, toda vez que, deacuerdo con el artículo 82 del Reglamento de la Unión Europea (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, se establece el derecho de indemnización y responsabilidad el cual señala que toda persona que hay sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del Reglamento “tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos”. Esto será de manera general para todos los responsables o encargados que hayan intervenido en el tratamiento de datos y en todo momento tendrán responsabilidad directa a menos de que demuestren que no es de alguna forma responsable del hecho que caso el daño, así como de que tomó todas las medidas necesarias previas para evitar que el evento de daño se diera a lugar por alguna omisión de su parte.

[51] El propio reglamento ofrece procedimientos específicos para los dos primeros incisos, que eran necesario que la legislación Española implementara a la brevedad para su debido cumplimiento con la UE, con respecto al tercer inciso, el gobierno Español identificó la necesidad de adaptar las sanciones y procedimiento de una forma que resultará equiparable los procedimientos de sus nacionales, con los de cualquier otro ciudadano de otro país miembro de la propia UE.

capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones".

La AEPD actuaba directamente de acuerdo a lo establecido en la ley 15/1999 y su propio estatuto y los puestos de trabajo que componen la agencia son desempeñados por funcionarios de la administración pública, sin embargo, con plena independencia de la administración pública.

Dentro de las funciones de la AEPD, de acuerdo a los propios lineamientos de la ley orgánica 15/1999 dentro de su artículo 37, se establecen los siguientes:

- Velar sobre el cumplimiento del reglamento.
- Atender toda clase de reclamaciones que provengan de la parte afectada en sus datos personales.
- Ofrecer información directamente a las personas que deseen conocer sobre el tratamiento y salvaguarda de sus datos personales.
- Requerir a los responsables, previa audiencia, las medidas necesarias para la adopción adecuada de medidas para la protección de los datos personales que recaba.
- Velar por el cumplimiento de todo el reglamento 15/1999 y de las disposiciones contenidas en La Ley de Estadística Pública que se impone para la debida recolección de datos estadísticos y al secreto estadístico de España.

Durante varios años, ésta fue la normatividad que se aplicó directamente en España, el origen de la creación de la Ley reglamentaria 15/1999 ha funcionado directamente de lo establecido en la directiva de la UE 95/46/CE, y durante varios años provocó que se acataran a su debido cumplimiento la ley. Inclusive "el derecho a controlar los datos que nos conciernen se concretan, como dice el Tribunal Constitucional español, en la atribución a las personas de un haz de facultades consistentes en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que se conocen como habeas data"[52].

[52] Garriga Domínguez, Ana, *op. cit.,* p. 8

Derivado de la reforma y aprobación del RGPD y de la nueva Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, la AEPD ha decidido aprobar una nueva normativa dentro de su organismo que permita realizar cambios sustantivos en su administración, permitiendo la implementación de facultades que permitirán una mejor aplicación del Reglamento.

Entre las modificaciones que el RGPD permite y que impacta directamente al comercio electrónico, es la facilidad que se les otorgará a los ciudadanos para que puedan ejercitar libremente sus derechos de protección de datos personales, y que los medios que utilicen para ejercitarlos sean de acceso fácil. Así mismo, dentro de los cambios que implementaron derivado del Reglamento, se les permite a los ciudadanos españoles que se les informe de una manera clara e inmediata del tipo de tratamiento que se les dé a sus datos personales y la facilidad de acceder a ellos a través de un acceso directo para su observancia y consulta.

Aquí es importante preguntarse: ¿cuál es la diferencia sustancial con lo regulado anteriormente por la AEPD? En este sentido, se considera que se da un paso significativo al reconocer directamente que estas medidas son diseñadas exclusivamente por actividades que deriven y/o que se realicen a través de Internet.

1.3. El valor social y económico de la información

La privacidad hoy en día se ha convertido en una fuente de atracción de clientes para empresas dedicadas al comercio electrónico; aquellas empresas que logran acaparar la atención de clientes quienes confían en comprar en línea porque consideran que su información será tratada adecuadamente y su privacidad será respetada, tienen una ventaja considerable frente a los que no ofrecen esa seguridad; este factor es importante para que el posicionamiento de empresas se ha considerado como un elemento de competitividad y de apoyo a un mercado único digital[53].

[53] El mercado único digital, un sector que abarca el marketing digital, el comercio electrónico y las telecomunicaciones, es un área sin fronteras donde las personas y las empresas pueden llevar a

Tal y como afirma De Pablos Heredero “La información es uno de los activos más importantes hoy en día de las organizaciones, y de manera especial para algunas compañías que operan en determinados sectores de actividad, en donde este recurso se convierte en crítico”[54]. En un futuro, se podrá visualizar a la gestión de la información como una de las herramientas más importantes con que contarán las empresas para poder tener ventajas competitivas frente a otras organizaciones, el b*ig data* pasó a tener una relevancia importante en el sector empresarial porque permite medir el verdadero valor de la información, un uso adecuado de programas de gestión de información es la diferencia entre una empresa y otra para generar valor económico.

Algunas de las nuevas formas en que se ha comenzado a conformar con la llamada economía digital es a través de la forma en que se emplean los datos y las finalidades de las mismas, entre otras cosas se puede considerar que los datos son el nuevo producto para muchas empresas, quienes a través de las estadísticas por medio del *Big data* conocen de manera sistemática y detallada la rentabilidad de los productos y/o servicios que ofrecen.

El comercio electrónico es un claro ejemplo de lo mencionado en el párrafo precedente, la base del comercio electrónico es la información, la cual puede llegar a partir desde la operación de transacciones figuradas a través de datos, así como de derechos intelectuales, tecnologías de la información y recursos que no pueden llegar a ser materializados como tal. “El consumo y el comercio electrónico son elementos centrales para el presente y futuro de la economía”[55]

Camacho Rodríguez señala al respecto el beneficio que ha traído consigo el comercio electrónico dentro de la economía digital, señalando como principales figuras la producción especializada de mercancías y la flexibilidad para su

---

cabo actividades comerciales, innovar e interactuar de forma legal, segura y a un coste asequible, haciendo sus vidas más fáciles. Significa que las empresas pueden hacer pleno uso de las nuevas tecnologías; y las pequeñas empresas, en particular, pueden atravesar la UE con un solo clic.

[54] De Pablos Heredero, Carmen, *et al*, *Organización y transformación de los sistemas de información de la Empresa*, 4ª. ed., Madrid, ESIC, 2019, p. 125.

[55] Camacho Rodríguez, Karla Teresa, “Reflexiones sobre la importancia de la noción de la clase social en los estudios de consumo. La relación de los jóvenes con las e-compras en México”, *Intersticios Sociales*, Guadalajara, año 9, núm. 17, marzo- agosto 2019, p. 77.

transportación de un lugar a otro, sin que las fronteras sean una limitante para el conocimiento de ese producto o su llegada al destino final, “también porque ahora es posible recabar una gran cantidad de datos sobre los gustos, interacciones, intereses y necesidades de las personas”[56]. La autora toma como base el avance que ahora existe en la forma en que puede conocerse a los consumidores, toda vez que a través de la información que proporcionan durante una transacción mercantil, se puede conocer los gustos de ese consumidor en especial y adaptar ciertos mecanismos que permitan transformar la experiencia de las compras y los negocios. Es importante señalar que aunque muchas veces la practica citada tenga como único objetivo conocer los gustos del consumidor, se ha llegado a utilizar la información para fines completamente diversos para lo que fueron recabados, por motivo de lo anterior, es que los países más activos en temas relacionados con la economía digital, como es el caso de Europa, han desarrollado legislaciones que se proponen acabar con el mal uso de la información.

Las reformas en materia de protección de información que en últimas fechas se han incorporado con la aparición del reglamento de la UE denominado RGPD, ha hecho que se renueve la forma en cómo debe de tratarse y controlarse la información de carácter personal.

El reglamento tiene como finalidad por primera ocasión el que se realice de manera objetiva y real una adecuada regulación en materia de protección de información por parte del sector privado, principalmente por los proveedores de servicios que a través de Internet realizan sus principales actividades que generan ingresos económicos.

La reforma en materia de protección de datos tiene unos objetivos precisos y hasta cierto punto considerados como drásticos; tal y como señala Fuensanta “se abandonan los instrumentos armonizadores en favor de los unificadores como el reglamento comunitario, apostando por el fomento de las TICs como una

[56] *Ibidem*, p. 68.

política europea horizontal que afecta a todos los sectores económicos y al sector público"[57].

Esto se debe en gran medida a los cambios digitales que la sociedad ha venido considerando y experimentando en aras del cambio, la llamada cuarta revolución digital ha comenzado a plasmar los principales sociales, en la forma en la que se utiliza y trata principalmente la información. Con estos cambios sociales y culturales se han considerado cambios en materia de comercio, tal es el caso de los llamados elementos de la economía digital:

1. Economía colaborativa. Consistente en la interacción entre dos o más sujetos a través de medios digitales y que tienen con objetivo crear lazos de comunicación para crear productos y servicios para una determinada sociedad y con un fin común y productivo para los mismos colaboradores. Este modelo de economía es de los más funcionales y atractivos para los usuarios, ya que se considera que no el limitante únicamente a productos y servicios, sino a fines diversos.
2. Intercambio gratuito de bienes y servicios.- También denominada economía social y solidaria en la consistente en el intercambio de productos y servicios de manera recíproca y sin obtener ventajas precisamente lucrativas, este tipo de economía tiene la particularidad de que lo que se recibe, solo debe de utilizarse y devolverse, sin que se conserve o se cambie de dueño.
3. Economía del trueque.- El cual consiste en intercambiar productos y servicios, sin que intervenga como tal el valor de las monedas o alguna forma, aquí los productos llegan a tener toda la carga económica, que se necesita para adquirir otros bienes y servicios.
4. Economía bajo demanda.- Este nuevo sistema de economías se dedican a transformar la manera en cómo se ofrecen los servicios en las empresas, esta economía en particular se dedica a "conectar al cliente directamente

[57] Fuensanta Martínez, Martínez, Dolores, "Unificación de la protección de datos personales en la Unión Europea: desafíos e implicaciones", *El profesional de la información*, Murcia, vol. 27, núm. 1, pp. 185-194.

con el prestador de servicios. De esta forma, estas compañías desarrollan su principal actividad a través de trabajadores autónomos"[58]

Lo que tienen en común estos nuevos tipos de economías es que materializan su existencia por medio de la economía digital o economía de la información, la cual tiene como principal objetivo que el mercado sea la información como tal. De acuerdo con lo señalado por la autora Fuensanta:

> Los datos y la información representan el principal factor de producción de un mercado digital anclado todavía sobre la teoría económica de los mercados bilaterales basados en la publicidad. El tratamiento de la información y de los datos mediante técnicas de profiling (elaboración de perfiles online de los usuarios) a partir de las cookies u otras técnicas de recopilación de datos proporciona la segmentación requerida por una publicidad comporta mental online[59]

El nuevo mercado de comercio que abrió la información, hizo que las leyes se vieran en la necesidad inminente de renovarse y en crear nuevas formas de regulación legislativa, que permitiera la existencia una protección integral para los titulares de la información que se comparte a través de medios electrónicos.

Por otro lado, al contemplarse una nueva forma de productos, "se ha llegado a afirmar que sus usuarios no son clientes sino productos, toda vez que la esencia del negocio de la red social se encuentra en los datos e información que los usuarios proporcionan y hacen públicos en sus perfiles"[60], por lo que, cada vez es más fácil entrar a algún tipo de estas economías pueden señalarse como colaborativas, gratuitas o de trueque, catalogándola de manera errónea.

Por tal motivo, el RGPD implica una serie de modificaciones con la intención de implementar estos cambios económicos, sin embargo "pese a su persistente objetivo de garantizar una protección uniforme y coherente en el

---

[58] Todolí Signes, Adrián, "La regulación especial del trabajo en la Gigeconomy", *Redes.com*, 2017, Núm. 15, *http://revista-redes.hospedagemdesites.ws/index.php/revista-redes/article/view/502/535*

[59] Fuensanta Martínez Martínez, Dolores, "Unificación de la protección de datos personales en la Unión Europea: desafíos e implicaciones", *El profesional de la información*, Murcia, vol. 27, núm. 1, pp. 185-194.

[60] *Idem*

tratamiento de los datos personales en la Unión Europea que fomente la libre circulación de éstos, presenta limitaciones o excepciones"[61]

Se considera que uno de los principales problemas de integración que experimentan las autoridades destinadas a la protección de información, es que no termina de definirse adecuadamente hasta la fecha el estatus que guardan este tipo de empresas, toda vez que este tipo de empresas quienes apenas están comenzando a regularse en materia de protección de datos aseguran que no pueden considerarse como empresas de comercio electrónico, ya que su objeto social es distinto al del intercambio de productos de bienes a cambio de una contraprestación por medios electrónicos.

Comienza a existir jurisprudencia que señala que este tipo de empresas que alientan la economía colaborativa, economía del trueque, economía bajo demanda, y la economía social, también pueden llegar a ser consideradas bajo el mismo esquema de que las empresas dedicadas al comercio, sin embargo, se ha estimado que depende a sus objetivo, llegan a ser consideradas completamente dentro del ámbito del comercio electrónico.

Uno de los temas más relevantes al respecto fue la cuestión prejudicial que se dio a conocer al Tribunal de Justicia de la UE.

El Tribunal de Justicia (Gran Sala) de 20 de diciembre de 2017 tuvo vista a una cuestión prejudicial planteada por el Juzgado de lo Mercantil número 3 de Barcelona, se ventiló el caso entre la *Asociación Profesional Elite Taxi* y*Uber Systems Spain, S.L.*con respecto a la sentencia C-434/15.

En el procedimiento prejudicial se estudió lo respectivo al artículo 56 TFUE, el artículo 58 TFUE, el apartado 1 Servicios en el ámbito de los transportes, la Directiva 2006/123/CE, los servicios en el mercado interior, la Directiva 2000/31/CE y la Directiva 98/34/CE de Servicios de la Sociedad de la Información. En dicha cuestión, se realizó una revisión de los alcances que jurídicos que tiene un servicio de intermediación, que permite mediante una aplicación para teléfonos inteligentes, conectar a cambio de una remuneración a conductores no

[61]*Idem*

profesionales que utilizan su propio vehículo con personas que desean realizar desplazamientos urbanos.

A través de la sentencia señalada con antelación, se le condena a *Uber*[62] que cumpla como un servicio de intermediación como integrante de servicios de transporte, no así como una aplicación de la libre aplicación prestación de servicios en general o como parte del comercio electrónico, toda vez que con sus objetivos de negocio, encajan perfectamente con los objetivos de una empresa dedicada al transporte, independientemente de los medios que utilice para tales efectos. El fallo es el que me permito transcribir a continuación:

> Fallo El artículo 56 TFUE, en relación con el artículo 58 TFUE, apartado 1, el artículo 2, apartado 2, letra d), de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006, relativa a los servicios en el mercado interior, y el artículo 1, punto 2, de la Directiva 98/34/CE del Parlamento Europeo y del Consejo, de 22 de junio de 1998, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas y de las reglas relativas a los servicios de la sociedad de la información, en su versión modificada por la Directiva 98/48/CE del Parlamento Europeo y del Consejo, de 20 de julio de 1998, al que remite el artículo 2, letra a), de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), deben interpretarse en el sentido de que ha de considerarse que un servicio de intermediación, como el del litigio principal, que tiene por objeto conectar, mediante una aplicación para teléfonos inteligentes, a cambio de una remuneración, a conductores no profesionales que utilizan su propio vehículo con personas que desean efectuar un desplazamiento urbano, está indisociablemente vinculado a un servicio de transporte y, por lo tanto, ha de calificarse de «servicio en el ámbito de los transportes», a efectos del artículo 58 TFUE, apartado 1. En consecuencia, un servicio de esta índole está excluido del ámbito de aplicación del artículo 56 TFUE, de la Directiva 2006/123 y de la Directiva 2000/31[63].

En virtud de lo anterior, se considera que más allá de que si se determina que la forma en la que se realizan transacciones comerciales, se cumple con una

[62] En 2009, Uber surgió como una nueva opción de transporte, revolucionando dicha industria con su modelo de negocio basado en una plataforma tecnológica cuyo principal fin es conectar conductores y pasajeros a través de una App. Es entonces que, desde su fundación en la ciudad de San Francisco, se ha expandido rápidamente a 65 países y 600 ciudades, véase Caro González, Arianis Suzeti, et al, *Plan estratégico de la Empresa Uber 2019-2023*, Lima, Trabajo de Investigación presentado para optar al Grado Académico de Magíster en Administración, 2019.

[63] Fallo El artículo 56 TFUE, en relación con el artículo 58 TFUE, apartado 1, el artículo 2, apartado 2, letra d), de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo.

disposición elemental, el intercambio de información, y toda vez que la información es considerada como un activo para crear relaciones que terminan en fines comerciales, los problemas que pueden derivar de los mismos, como la perdida de información, infiltración y/o robo de datos, éstos independientemente del estatus legal bajo el que se encuentren constituidos, serán responsables directos de su cuidado y protección.

Sin perjuicio de lo anterior, es menester considerar que una empresa dedicada a este sector como *Uber*, y al ser considerado más allá de un intermediario, no le quita sus responsabilidades como dicho intermediario de información. Los intermediarios han comenzado a crear algunas ideas que permiten controlar la información y permiten que sea una forma segura de venta para que la relación con sus clientes, no causen incertidumbre.

Por un lado la recolección a grandes escalas de información y datos, han hecho que se cambie la forma en la que se le da tratamiento a la información, toda vez que en la mayoría de las ocasiones, las mismas operaciones permiten que se procesen, se analicen y se crucen los datos unos con otros y en muchas ocasiones intervienen más de alguna persona en ese proceso. Tal y como afirman las autoras Navas Navarro y Camacho Clavijo “En esta dirección, intervienen no solo el responsable del mismo, sino también encargados y sub encargados, con lo cual, existe una cadena de subcontrataciones. Incluso, el propio usuario final puede ser considerado, en determinados casos, responsable del tratamiento de los datos”[64].

Lo anterior permite reflexionar la importancia del control y gestión adecuada de la información, sin importar el estatus con que cuente el poseedor de la información, se puede definir que todos los involucrados, en algún punto tendrán responsabilidad completa o compartida de la protección de la información, por lo que deberán de definirse sus claramente las obligaciones de cada uno de ellos para que se tomen medidas adecuadas de protección.

[64]Navas Navarro, Susana y Camacho Clavijo, Sandra, *Mercado digital, principios y reglas jurídicas*, Valencia, Tirant lo Blanch, 2016, p.57.

CAPÍTULO 2
LA PROTECCIÓN DE DATOS PERSONALES EN EL COMERCIO ELECTRÓNICO

SUMARIO: 2.1. *El comercio electrónico y sus principios básicos*; 2.2. *Evolución histórica del comercio electrónico*; 2.3. *El comercio electrónico como herramienta para el proceso de transformación de la economía digital; 2.4.La protección de datos personales en el comercio electrónico; 2.5. Elementos comparativos a la normativa jurídica del derecho, derivados del e-commerce en México y la Unión Europea.*

En el presente capítulo se podrá apreciar el avance histórico que ha tenido el comercio electrónico, partiendo desde sus principios básicos hasta las definiciones legales que se le han proporcionado en diversos países, incluido México; así como la percepción que varios autores y organizaciones tienen de él en la actualidad. Así mismo, se podrá apreciar la transición de los actos mercantiles tradicionales a las nuevas prácticas utilizando las tecnologías de la información, para así, comprender la importancia de su estudio e implementación en la vida cotidiana.

2.1. El comercio electrónico y sus principios básicos

A partir del surgimiento del llamado Internet, se han suscitado una serie considerable de cambios en la sociedad y la forma en la que se relacionan, el comercio electrónico fue una de las actividades que se transformaron con las TICs.

El comercio electrónico se puede definir de formas diversas y depende en reiteradas ocasiones por los elementos que la componen y los autores que han

interpretado su objetivo.

Desde el punto de vista publicitario para autores como Martínez Valverde y Rojas Ruiz, el *e-commerce* es "la aplicación del marketing en Internet sobre la que se confluirán los esfuerzos realizados de las empresas en el resto de las áreas"[65]

En otro sentido, tal y como señala el autor Andrés Blasco, "el comercio electrónico ocupa un espacio en el ámbito de Internet donde la seguridad es imprescindible para su normal funcionamiento"[66]

De acuerdo con algunos autores, el comercio electrónico se define como el acto de realizar transacciones comerciales a través del uso de medios electrónicos. Sin embargo, de igual forma hacen la importante aclaración que "la mayoría de las veces hace referencia a la venta de productos por Internet, pero el término comercio electrónico también abarca mecanismos de compra por Internet (de empresa a empresa)"*[67].*

Por su parte, José María Antemporlatinam define al comercio electrónico como "aquel que consiste en el desarrollo de una actividad comercial, con multiplicidad de operaciones, que se puede realizar por vía telemática (electrónica) y basada en la cesión de productos, prestación de servicios e intercambio de datos (información), pudiendo realizarlos en tiempo real"*[68]*.

Para Ignacio Somalo, el comercio electrónico "significa el traslado de transacciones normales, comerciales, gubernamentales o personales a medios computarizados vía redes de comunicaciones, incluyendo gran variedad de actividades"[69].

Entes gubernamentales como la Organización Mundial del Comercio, definieron al comercio electrónico desde septiembre de 1998 en su programa de

---

[65] Martínez Valverde, José Fulgencio y Rojas Ruiz, Fernando, *Comercio electrónico*, Madrid, Paraninfo, 2016, p. 7.

[66] Andrés Blasco, Javier de, "¿Qué es el internet?", en García Mexia, Pablo (director), *Principios de derecho de internet*, 2ª ed., Valencia, Tirant lo Blanch, 2005, p. 76.

[67] Pillou, Jean-François, *Introducción al comercio electrónico (e-Commerce)*, junio 2017, *http://es.ccm.net/contents/201-introduccion-al-comercio-electronico-e-commerce.*

[68] Antemporlatinam Valero, José María, "Definición de comercio electrónico", *Relevancia del Ecommerce para la empresa actual*, Valladolid, tesis para obtener el grado de doctor, 2014, p.12.

[69] Somalo Peciña, Ignacio, *El comercio electrónico: una guía completa para gestionar online*, Madrid, ESIC, 2017, p.16.

trabajo como “la producción, distribución, comercialización, venta o entrega de bienes y servicios por medios electrónicos”[70]

Dentro de algunas definiciones atendiendo a la finalidad del comercio electrónico, se señala que “el comercio electrónico es un canal de distribución con un enorme potencial, con grandes beneficios para los vendedores y consumidores, ya que puede generar ahorros, al permitir a las empresas reducir costos, al no necesitar gastos de arrendamiento y mantenimiento a los locales”[71]

Por otro lado, para autores como Karina Velázquez, hay varias formas de denominar a la actividad encargada de intercambiar productos y/o servicios a través del uso de medios electrónicos, para ella las denominaciones de *Ecommerce, E-commerce, E Commerce o E- Business*, son sinónimos y utilizar una u otra denominación, se considera como un término correctamente aplicado.

De lo anterior se deduce que el comercio electrónico no debe de interpretarse únicamente como un tipo de operaciones o transacciones de las diversas especies de productos o servicios, sino como una forma de transacción de información a través de medios electrónicos específicos, y para que lo anterior surta plenos efectos, que estas transacciones requieran de las tecnologías de la información para cumplir con su objeto; claro está, que, aunque de forma general se englobe a cualquier medio electrónico, el telégrafo, el teléfono, el fax o la televisión, generalmente se asocian únicamente los medios electrónicos y los derivados del Internet.

Sin perjuicio de las definiciones mencionadas y atendiendo a la interpretación legal propia del comercio electrónico, algunos autores como Pendón Meléndez en su obra *La perfección del contrato en Derecho Privado*, han definido a esta nueva forma mercantil de creación de relaciones comerciales como contratación electrónica. Para el autor, es más adecuado revisar este ámbito del derecho con esa denominación, toda vez que, consideraba necesario que se

---

[70] Organización Mundial del Comercio*, Comercio electrónico, 2017, https://www.wto.org/spanish/tratop_s/ecom_s/ecom_s.htm.*

[71] Valdés Hernández, Miguel Ángel, “Diagnóstico del comercio electrónico con base en la confianza, seguridad y conocimiento del consumidor final”, *Red internacional de investigadores en competitividad*,México, vol. 8, núm. 1, 2014, p. 677, *https://www.riico.net/index.php/riico/article/view/1177/845.*

revisara la normativa vigente en la época hasta ese momento y, que a partir de eso, se restablecieran las condicionantes que permitieran una mejor compresión de los objetivos del nuevo tema a legislar; tal y como el autor señala "de esta forma, podrá prestarse más atención a lo esencial (los fundamentos y los fines de regulación), antes que a lo accesorio (cada una de las diversas técnicas sobres las que se pretenda asentar o aplicar la reflexión sobre las normas legales)"[72]. Para él, este tipo de trabajos tiene como finalidad dar una revisión necesaria al derecho que durante varios siglos se ha ido creando y regulando, para poder hacer una comparativa y reflexionar de su significado con el ahora futuro que se está construyendo en la actualidad, refiriéndose en tal sentido a los medios tecnológicos que han estado ganando terreno en la sociedad del siglo XXI, es decir, para él, no es intención del legislador, como más adelante se observa en los principios de la contratación electrónica, de tratar de crear nueva legislación enfocada a los nuevos tipos de comercio, ya que el comercio desde épocas milenarias se ha ido creando y definiendo a través de bases ahora sólidas y bien identificadas por el Derecho, tal es el caso de la llamada confianza, los productos o servicios o la actividad que tiene por objetivo el intercambio de productos o servicios por una cantidad identificada, "no se trata simplemente de un cambio de denominación, sino sobre todo de un cambio de orientación"[73]

En Europa el comercio electrónico se ha investigado con el propósito de crear normativa que regule los principales problemas que, hasta la fecha han derivado de la práctica común entre las actividades del comercio en la red, pero también ha llegado a la conclusión de que aunque se trata de una forma de comercio relativamente nueva, adecuándose a las tecnologías que han dado lugar a nuevas formas de realizar el comercio, los enfoques y las finalidades sustanciales del tema no han cambiado, es decir, por ningún motivo se trasponen de la forma en la que, a lo largo de los años, se han estado llevando a cabo actividades mercantiles. Tal y como señala Pendón Meléndez, quien a la letra señala:

[72] Pendón Meléndez, Miguel Ángel, *La perfección del contrato en Derecho Privado*, Valencia, Tirant lo Blanch, 2009, pp. 70-71.
[73] *Ibidem*, p. 71.

> …En algunos casos sí ha sido imprescindible la creación de normas *ad hoc*, pero no es esta una exigencia del Derecho Privado, al menos en el ámbito de las declaraciones de la voluntad y de su expresión, comunicación y documentación, en la que muchas veces es obviado principio espiritualista que preside en buena medida sus relaciones se ha visto innecesariamente reafirmado en normas[74].

Lo anterior lleva a reflexionar y concluir, que no debe de ser intención ni finalidad principal del derecho el querer regular algo que por naturaleza se ha estado realizado por miles de años con una finalidad principal, el comercio desde épocas remotas ha dado lugar a un mismo fin, que ha sido el del intercambio de productos o servicios por precio determinado, el que ahora se hayan implementado nuevas formas en las cuales esos actos de comercio se lleven a cabo, nunca deben de quitarnos la idea clara de que la finalidad del comercio, se sigue llevando a cabo en el comercio electrónico, y que no es importante mediante qué medios se realice, siempre y cuando no se altere la finalidad. En líneas expresadas más adelante podrán apreciarse los tres principios del comercio electrónico, sobre los cuales, se han sentado las bases de regulación y que han ayudado a la compresión de las verdaderas necesidades jurídicas que al día de hoy son importantes cuidar.

2.1.1. Principio de equivalencia funcional

El comercio electrónico asienta sus bases en tres principios reconocidos internacionalmente por la comunidad del Internet y del comercio, en los cuales han participado innumerable grupos de expertos en la materia, que han llegado a una misma conclusión, el Internet solo cambia la forma en la que se realiza el comercio, no su esencia ni su finalidad.

Ley Modelo de la CNUDMI sobre el Comercio Electrónico expresa la siguiente posición:

> En el principio de la equivalencia funcional se establecen los criterios conforme a los cuales las comunicaciones electrónicas pueden equipararse a

[74]Pendón Meléndez, Miguel Ángel, *La perfección del contrato en Derecho Privado*, Valencia, Tirant lo Blanch, 2009, p. 74.

las comunicaciones sobre papel[75].
…En particular, enuncia los requisitos concretos que deben cumplir las comunicaciones electrónicas para realizar los mismos fines y desempeñar las mismas funciones que se persiguen en el sistema tradicional basado en el papel con determinados conceptos, como los de *escrito, original*, *firma*, y *documento*.[76]

Por otro lado, Polanco López argumenta que "el principio de equivalencia funcional procura que la información en forma de mensaje de datos tenga reconocimiento jurídico en similares términos a sus homólogos del comercio tradicional"[77]

Los elementos que han perfeccionado este principio, tienen como finalidad equiparar los efectos jurídicos que tiene un mensaje tradicional escrito y un mensaje electrónico, las finalidades perseguidas en este caso en concreto son las mismas, como puede ser una oferta y una aceptación de la misma.

A través de los aspectos que se fueron identificando y analizando dentro del comercio electrónico, los estudiosos del derecho se plantearon varias cuestiones que era necesario definir para comparar y finalmente decidir que el comercio electrónico, no se transponía en ninguna forma con el comercio tradicional como acto mercantil, algunas de las cuestiones tratadas fueron las siguientes:

- El comercio electrónico y el comercio tradicional no necesariamente tienen que ser idénticos. Sólo deben de cumplir con la misma finalidad
- La formalidad de un contrato de comercio no cambia, toda vez que cuándo en los Códigos de Comercio se señala "deberá firmarse por la partes" significa:

  a) Aceptar, expresar conocimiento. Manifestar un consentimiento

  b) Identificar a la persona.

  Por lo que se acepta un contenido identificado a través de los siguientes

75 Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996), consultado el 7 de noviembre de 2018, *http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/1996Model.html*

76 *Idem*

77 Polanco López, Hugo Armando, *Manifestaciones del principio de equivalencia funcional y no discriminación en el ordenamiento jurídico Colombiano*, Santiago de Cali, Criterio Jurídico, 2017, p.43.

medios:

a) Huella en el teléfono.
b) Firma en un correo electrónico.
c) Pin de una tarjeta electrónica.

- En derecho cambiario está el llamado derecho al portador. ¿Cuál es la posesión en el Internet? La posesión es una posesión exclusiva intangible, no importa si son papeles o datos, porque solo uno mismo conoce la clave.

Uno de los textos legales más significativos y reconocidos internacionalmente, los cuales tratan directamente las cuestiones prácticas de la equivalencia funcional es la Ley Modelos de la CNUDMI, en el cual, en su artículo 6º se expresa el reconocimiento de este principio, como si se tratará de un principio de literalidad de un escrito "centrado en el concepto básico de la información que se reproduce y se lee"[78], por lo que se llega a la conclusión que, mientras se disponga de cierta información para su posterior consulta, sin importar el medio o soporte en el que se almacene, debe de interpretarse con las mismas finalidades y efectos.

2.1.2. Principio de neutralidad tecnológica

La neutralidad de la red, es referida por autoras como Navas Navarro y Camacho Clavijo como "un principio que garantiza la comunicación universal, abierta a todos los participantes, sin discriminación. Los usuarios pagan por conectarse a la red y el precio depende de la velocidad y calidad de la conexión que deseen"[79]. De acuerdo esta definición, la información que es tratada en la red, es decir, el conglomerado de datos que se encuentran distribuidos y contratados por los usuarios, debe de ser la misma, por lo que el nivel de calidad y medidas de

[78] Polanco López, Hugo Armando, *Manifestaciones del principio de equivalencia funcional y no discriminación en el ordenamiento jurídico Colombiano*, Santiago de Cali, Criterio Jurídico, 2017, p.49.
[79] Navas Navarro, Susana y Camacho Clavijo, Sandra, *op. cit.*, p.58.

seguridad deben de ser iguales en cualquier lugar donde se distribuyan.

En relación con las autoras anteriormente citadas, la red debe de ser un medio abierto, distribuido y de acceso universal y para ellas debe de mantenerse siempre así, a pesar de los intentos de los prestadores de servicios de ser ellos mismos quienes gestionen y autoricen el tráfico y acceso a la información[80]; sin embargo, es importante hacernos la interrogante de ¿qué es lo que sucede cuando la información distribuida vulnera algún derecho de algún tercero? O cuándo la confidencialidad de una persona se ve trastocada frente a la invocación de tal principio. Es claro que se está de acuerdo parcialmente con tal principio y que mientras recoja las finalidades principales para el que fue creado, está bien; pero no hay que olvidar que como toda norma, existen sus excepciones que deben de ser contempladas y reguladas de manera particular a casos concretos.

En este sentido, varios han sido los organismos internacionales preocupados por la regulación de este tema. Por su parte Estados Unidos a través de la FCC[81], ha señalado que es importante la creación de una red abierta y que se señale a los proveedores de servicios que no debe de existir, bloqueo discriminación y transparencia[82], opinión similar a lo que se ha estado trabajando en el marco de la UE tratando de evitar el falseo de la información y en la cual, se trata fomentar a su vez, la interconectividad de extremo a extremo garantizando la igualdad y la no discriminación[83].

[80] *Idem*

[81] La FCC actúa como la reguladora de las todas las comunicaciones de los estados de Estados Unidos, incluyendo el distrito de Columbia, por cualquier medio incluyendo la radio, televisión, cable y satélite, establece alto criterio en el derecho de las telecomunicaciones y en general en la innovación tecnológica.

[82] Navas Navarro, Susana y Camacho Clavijo, Sandra, *op. cit.,* p.59.

[83] En tal sentido, se hace referencia a la *Propuesta de Reglamento del Parlamento europeo y del Consejo,* por el que se establecen medidas en relación con el mercado único europeo de las comunicaciones electrónicas y para crear un continente conectado.

2.1.3. Principio de no alteración del derecho pre-existente (o Principio de subsistencia)

Este principio se basa principalmente en la hipótesis de que con las TICs se ha llegado a nuevas formas en que puede almacenarse, demostrarse y transmitirse la voluntad de las partes, que es lo más importante para que un acto de comercio pueda llevarse a cabo, sin embargo, el que se creen estas nuevas formas de manifestación de la voluntad, no quiere decir que tenga que variar algo más por lo que deba de considerarse diferente al comercio electrónico del comercio tradicional.

Entre algunos de los organismos que se han encargado de regular el comercio internacional y, principalmente, el comercio electrónico, es la CNUDMI, organismo que por el cual, a través de la elaboración y creación de leyes modelo y de normativas que permiten una reguladora participación entre los países que intervienen en temas del comercio mercantil, este organismo ha sido un marco de referencia a lo largo de los años. A pesar de eso, se ha llegado a la aseveración de que estas nuevas formas, no cambian en ningún sentido el derecho establecido desde hace varios siglos atrás.

> Circunscrita a ese ámbito de las telecomunicaciones, la electrónica no exigiría cambios normativos en materia de contratación (celebración, perfección y ejecución de los contratos privados). Ello no es incompatible con la necesidad de especialidades operativas (que no conceptuales, esto es, acerca de las correspondientes instituciones), que, adaptando el sistema garanticen la seguridad requerida (la confianza vendrá, lógicamente, después, cuando el sistema me muestre efectivo y seguro[84].

Con lo anterior, se da un panorama de reconocimiento hacia diferentes formas en las que un acto jurídico puede llevarse a cabo, gozando con la garantía de validez que el Derecho solicita. Los actos celebrados por medios electrónicos deben de ser reconocidos en todo momento, con la misma fuerza legal que los actos celebrados por medios tradicionales, tal es el caso de los celebrados en papel, es necesario comprender y adaptarnos a los cambios que la tecnología ha traído, sin que el derecho sea un obstáculo cumplir con las finalidades propuestas.

[84]Pendón Meléndez, Miguel Ángel, *op. cit.,* p. 78.

2.1.4. Principio de la no discriminación

Un principio adicional, que más allá de que aplique únicamente al comercio electrónico, aplica para la actualidad a cualquier elemento de prueba que en Derecho pudiera invocarse a la hora de hablar de la validez de un documento, de acuerdo con la Ley de la CNUDMI sobre el comercio electrónico "el principio de la no discriminación asegura que no se denegarán a un documento sus efectos jurídicos, su validez o su ejecutabilidad, por la única razón de que figure en formato electrónico"[85].

Se ha llegado a equiparar el principio de No discriminación con el principio de equivalencia funcional, toda vez que se establece a la par para determinar que los mensajes de datos y las formas de expresión de la comunicación deben de contar los mismos grados de validez para que su finalidad sea realizada; sin embargo, estos principios tienen que ser aislados, considerando a la equivalencia funcional con las nuevas formas de contratación a través de medios electrónicos y al principio de No discriminación, con aceptación de los hechos que nacen de esos actos jurídicos, sin importar los medios que se empleen.

2.2. Evolución histórica del comercio internacional electrónico

El transcurso del tiempo y la forma en que la sociedad ha venido evolucionando, principalmente por los avances tecnológicos, es la razón por la que la forma en que se realizan varias actividades de la vida diaria, han sufrido un cambio considerable en la forma en que se llevan a cabo, el comercio no ha sido una excepción.

Actualmente, la sociedad interactúa con herramientas que TICs, principalmente el Internet, han proporcionado, y que han modificado sustancialmente la forma en la que se desarrolla la vida habitual de las personas. En la era actual, la mayor parte de las actividades diarias se realizan frente a una computadora, la cual permite mantener conversaciones, crear identidades,

[85] Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996), *op. cit.*

interactuar y precisamente el tema de este estudio de la presente investigación, el realizar relaciones comerciales, razón de lo anterior, se considera pertinente hacer una mención especial a esta red digital de comunicación.

Tal y como lo señala Manuel Castells “Internet es el tejido de nuestras vidas en este momento. No es futuro. Es presente. Internet es un medio para todo, que interactúa con el conjunto de la sociedad y, de hecho, a pesar de ser tan reciente, en su forma societal”[86]. Y aunque el tema sea relativamente nuevo en nuestra sociedad, con apenas aproximadamente 35 años desde las primeras apariciones del Internet, ha logrado que de manera rápida y contundente comenzara a implementarse como una nueva forma de vida.

En unos inicios se vio al Internet como una fuente de comunicación dirigida a las instituciones gubernamentales, militares y de investigación, se creó con la intención de tener una mejor y más rápida comunicación, permitiendo que las actividades diarias se realizaran de una manera eficaz y simple para las personas que pertenecían a esos grupos sociales. Sin embargo, con el paso del tiempo se descubrió que el Internet no era únicamente para manejar relaciones de tipo social, militar y político, se visualizó que podrían obtenerse otro tipo de ventajas a través de su uso.

A partir de prácticas comunes, como lo es el comercio, así como el descubrimiento de las tecnologías, es que de manera consuetudinaria fue surgiendo el comercio electrónico o *E-commerce*, como también se le denomina al acto de intercambio de productos y/o servicios a través de una contraprestación económica.

El comercio electrónico nació como una actividad dentro de la economía que tuvo sus inicios “en los años setentas, en los Estados Unidos y evolucionó hasta la forma en que lo conocemos hoy”[87], y aunque ese tipo de operaciones comenzaron varias décadas atrás, no fue sino hasta el año 2000 en que comenzó con un auge impresionante de expansión y afluencia económica.

---

[86] Castells, Manuel, *Internet y la sociedad red,* Barcelona*,* La Factoría, 2001, vol. 14, p. 1.

[87] Oropeza, Doris, *La competencia económica en el comercio electrónico mexicano y su protección en el sistema jurídico mexicano*, México, UNAM, 2018, p. 9.

Doris Oropeza, señala a la empresa *e-pages*[88]como una de las principales investigadoras del comercio electrónico, ya que ha llevado una investigación minuciosa de la evolución económica y tecnológica que ha llevado esta actividad con el paso de los años, razón de lo anterior, se ha divido hasta el día de hoy al *comercio electrónico* en cinco etapas a través de la historia[89]:

1. La pre-web. Entre la época de 1987 y 1992 aparece por primera vez la cuenta electrónica SWREG[90], en 1990 se crea la Assymetric Digital Subscriber Line[91], así como el primer sitio web del mundo en al año de 1991.
2. El lanzamiento de la web. De 1992 a 1997 nace el primer navegador web comercial nombrado *Mosaicm* que posteriormente cambiaría su denominación a *Netscape,* y años más tarde en 1995, con la creación del sistema operativo de Microsoft, se crean las primeras plataformas en línea para venta de productos, como lo fue *E-bay* y Amazon.
3. La era "puntocom". Entre los años 1997 a 2002 ya se registraban quinientos millones de usuarios de Internet y para 1997 la compañía *Dell* ya había registrado ventas en línea de más de un millón de dólares. Al finalizar esta época, se llegaron a registrar que tan solo en Estados Unidos, una de cada dos personas había comprado por Internet.
4. El nacimiento de Google. Entre los años 2002 a 2007 con el inicio de la plataforma de Google se comienzó a disparar la publicidad en línea, y ésta a su vez, en la principal fuente del comercio electrónico, por lo que para el año 2002 ya se había registrado que la mitad de la población de Estados Unidos ya había hecho su primera compra en línea, otros acontecimientos como la compra de *paypal* por *Ebay* en 2003, el lanzamiento de *Myspace* en 2003 y la creación de *Facebook* en 2004

[88] Proveedor independiente en Europa que crea software dedicado al comercio electrónico, el cual se especializa en crear soluciones tecnológicas en materia de comercio electrónico, por su amplia experiencia en la materia, ha sido considerada como una de las principales plataformas en el estudio de la evolución del mismo.
[89] Oropeza, Doris, *op cit*, p. 10.
[90] Empresa pionera en impulsar los pagos en línea.
[91] Innovación tecnológica que permitió el primer acceso a internet por medio de una banda ancha.

marcan esa época.

5. El regreso de *Apple*. En el año 2007 una de las principales empresas dedicadas al desarrollo de *software,* la empresa denominada *Apple* lanzó algunos de sus dispositivos más importante, el conocido *iPhone*, posteriormente para el año 2008 *Google* lanza *Android* y para el 2011, se registra que 8 de cada diez personas cuentan con teléfonos celulares. Lo anterior marca una verdadera revolución en el tema de las telecomunicaciones, y por ende la forma en que se llevan a cabo las principales operaciones y transacciones comerciales.

De igual forma, el comercio electrónico se ha clasificado de acuerdo con la actividad que ha realizado para llegar al público consumidor, "*Microsoft* concibe al comercio electrónico en dos grandes etapas: como el *e-commerce 1.0* y el *e-commerce 2.0.* La primera categoría habla de las empresas tradicionales que hacían uso de la Web solo para crear presencia en línea creando escaparates de sus productos, y finalizando la compra a través de una llamada telefónica o incluso invitando al cliente a asistir a su tienda física"[92]

Las empresas han sido las pioneras en incursionar al comercio electrónico por lo que han influido en los principales mercados electrónicos, son una fuente adecuada para que más personas obtén por incursionar en el comercio electrónico o para que obtén por comprar en línea.

Una de las compañías tecnológicas pioneras del comercio electrónico y que cuenta con gran auge y presencia entre las ciudades europeas, es la conocida como *Pixmanía*[93].

Esta compañía fue creada en Francia en el año 2000 con el objetivo de ofrecer a sus clientes un servicio de venta en línea de diversos productos, ya que lograron ofrecen a sus clientes, una variedad de productos incalculable y los precios más competitivos y accesibles, rápidamente fueron posicionándose en ese país y posteriormente se extendieron en más de 26 ciudades de Europa.

[92] Oropeza, Doris, *op cit,* p. 11.

[93] Martín, Javier, "Pixmania ocupa la calle", *El País*, Barcelona, 20 de marzo de 2012, *http://tecnologia.elpais.com/tecnologia/2012/03/20/actualidad/1332232088_282597.html.*

Cabe mencionar que esta empresa tiene total presencia en línea y ésta fue de las primeras empresas creadas con la intención de ofrecer a los consumidores precios económicos que dieran oportunidad de proporcionar un servicio en línea de calidad.

2.3. El comercio electrónico como herramienta para el proceso de transformación de la economía digital

Como se ha logrado transmitir en el presente capitulo, el comercio electrónico surgió de la creación de las tecnologías de la información y comunicaciones, las cuales han permitido que nuevas formas de comunicación se expandan y por consiguiente se consideren mayores posibilidades de comercializar productos y servicios. Lo anterior se dio como un hecho inevitable e irreversible, en virtud de que la gente comenzó a identificar rápidamente las ventajas que se obtenían de utilizar estas herramientas virtuales que permitían comunicarnos de una forma rápida, sin necesidad de realizar un esfuerzo mayor y llegando a un mayor número de personas.

En los primeros años de su creación, el Internet y posteriormente el comercio electrónico eran una fuente inaccesible y poco atractiva para su uso; simple y sencillamente la gente oía hablar de su existencia, sin embargo, se limitaba a hacer uso de estas herramientas o simplemente se convertía en un espectador que no obtenía ningún provecho de su existencia. Con el paso del tiempo esto ha cambiado radicalmente.

Tal y como lo menciona Gerardo Gariboldi, “En el contexto de tecnología digital, el comercio electrónico dejo de ser una oportunidad para convertirse en un requerimiento más a los fines de poder operar. Ya no es una opción sino una necesidad”.[94] Actualmente, se ha vuelto un estilo de vida; las nuevas generaciones han crecido con ellas y las ventajas significativas que se obtienen de su uso, hacen reflexionar que ya no hay paso atrás para dejar de operar sin ellas.

Esta práctica mercantil ha llegado a desplazar a los tradicionales métodos

[94] Gariboldi, Gerardo, C*omercio electrónico: conceptos y reflexiones básicas*, Buenos Aires, Instituto para la Integración de América Latina y el Caribe, INTAL, 1999, p. 1.

de comunicación y ventas, con respecto a esta última, se refiere principalmente a la generación de propagandas y publicidad por medios impresos, hoy, los comerciantes, grandes empresas y marcas, utilizan medios electrónicos, contra las llamadas telefónicas, visitas personales o la publicación de servicios por medios como los periódicos, revistas y volantes.

Actualmente, con la ayuda de los medios electrónicos se permite al comercio electrónico llegar a una mayor audiencia, en una velocidad de tiempo corta y facilitando ventajas de distribución a grupos sociales determinados que años atrás el comercio tradicional no permitía. Me permito citar lo aseverado por Gerardo Gariboldi al respecto.

> A nivel general, todo parece indicar que el comercio electrónico – al eliminar barreras y permitir un contacto en tiempo real entre consumidores y vendedores- producirá mayor eficiencia en el ciclo de producción trayendo esto aparejada la reducción de los costos, que, a su vez, se traduciría en una disminución de precios. Por otro lado, se eliminarían los intermediarios, aumentando la velocidad del ciclo comercial en su totalidad y constituyendo una nueva causa de ahorros.[95]

Antes de contar con estas herramientas de comunicación e interacción se obligaba a que los consumidores de un producto en específico realizara la búsqueda de éstos en forma personal; en la cual acudía directamente al establecimiento para ver si se encontraba el artículo de su interés, o un artículo lo más parecido posible, gastando tiempo y dinero en tal búsqueda; ahora con la ayuda del comercio electrónico se le da acceso a que con un solo *click* en cuestión de segundos acceda a una base de datos que le permite escoger entre una gran cantidad de artículos que desean o - en muchas ocasiones- que superan las expectativas de lo que en un inicio el consumidor busca. “lo cierto es que la tecnología redefinió las reglas de los mercados, planteando la posibilidad que nuevos competidores aparezcan constantemente, a velocidades nunca observadas”.[96]

Por lo anterior, el mercado global, en un primer plano, las empresas internacionales, han comenzado a implementar el uso de las tecnologías de la

[95] *Ibidem*, p. 9
[96] *Ibidem*, p. 10

información y comunicación para llegar a un mayor número de consumidores y lograr que sus activos crezcan significativamente.

2.4. La protección de datos personales en el comercio electrónico

El comercio electrónico es una nueva forma de negocios que basa su principal funcionamiento a través de la transferencia de información. El propio intercambio de información ha puesto en la mira de estudios, la idea de la importancia que representa todo el flujo de información que se transmite entre las partes a la hora de realizar una transacción mercantil, y sobre todo ha recocido la importancia de regular de manera nacional e internacional desde la esfera de cada uno de los países que interfieren en dichas transacciones.

2.4.1. En México

México ha comenzado a despegar en cuanto a protección de datos personales, con un propósito concreto, el tratar de posicionarse en la mira de otros países del mundo para abrir puertas de comunicación y expandir su mercado a ámbitos internacionales.

Con respecto a esa línea de comunicación entre México con otros países, se encuentra la relación entre éste y España y se ha llegado a afirmar que México es considerado un país atractivo para muchas empresas españolas para expandir su negocio, y viceversa, muchas empresas mexicanas ven en España una oportunidad y una puerta de entrada al mercado europeo.

Entre estos objetivos que se ha propuesto México en los últimos años, ha hecho que preste importante atención en uno de los recursos intangibles más importantes de hoy en día, como lo es los datos personales y la información que se maneja alrededor del mundo. Ya sea para relaciones de negocios o meramente políticas o diplomáticas, los países como España y México tratan datos personales para cualquier forma de comunicación y transacciones por lo que, México de manera particular ha realizado en los últimos años una serie de reformas legales

que permiten alcanzar una normativa aplicable que cubra las necesidades y proteja a ambos países.

A la fecha, México cuenta con una gran ventaja para llevar a cabo la finalidad de crear lazos comerciales con otros países, especialmente con España, toda vez de que ha hecho importantes modificaciones a su legislación para ofrecer una adecuada protección de datos personales; a la fecha México cuenta con una LFPDPPP, la cual se publicó en el *Diario Oficial* de la Federación el 5 de julio de2010, y posteriormente llevó a cabo la elaboración de su respectivo reglamento el día 21 de diciembre del año 2011. Es importante hacer mención que también que México ha sido el primer país en aprobar una ley de protección de datos tras la adopción de los Estándares Internacionales de Protección de Datos y Privacidad (Resolución de Madrid) en cual se llevó a cabo en el año 2009.

El que se haya llevado a cabo la Resolución de Madrid, permitió que México pudiera visualizar la necesidad que en materia de protección de datos se necesitaban a nivel internacional y para implementar en su propia legislación, por lo que cabo de la creación de la Ley de protección de datos.

Algunas de las principales similitudes con las que cuentan los dos países son los siguientes:

- España y México, dentro de la respectiva legislación que los regula cuentan cada uno con la protección de los principio de consentimiento, licitud, calidad, información y lealtad.
- Ambos protegen los derechos de Acceso, rectificación, Cancelación y Oposición, también conocidos como los derechos ARCO y estos a su vez, cuentan con las medidas administrativas para exigir su debido cumplimiento.
- Ambos países cuenta con unidades especializadas de protección, por un lado España cuenta con la AEPD y, por su parte, México cuenta con el Instituto Nacional de Acceso a la Información (INAI).
- Ambos países mantienen fidelidad con la protección de información a través de los avisos de privacidad que proporciona a sus principales

consumidores, sin importar la nacionalidad que tenga el consumidor final del producto y/o servicio a ofrecer.

México a través del INAI ofrece por medio de su portal en línea la guía para elaborar los avisos de privacidad, misma que ha denominado como el ABC del Aviso de Privacidad del INAI. Dicha guía entre otras cosas, enuncia los requisitos mínimos que deberá de contener la declaración de privacidad, haciendo gran énfasis en establecer de forma clara, precisa y no engañosa de qué tipo de información se recabará, con qué finalidades y en qué condiciones se mantendrá segura.

Los avisos de privacidad, al ser una herramienta que es utilizada en el plano internacional, han permitido que se transmita una confianza de México hacia otros países del mundo, lo que ha provocado que se amplíe la esfera comercial internacional.

Por otro lado, aunque las reformas a la legislación mexicana se hayan hecho en base a estándares internacionales, a la fecha cuenta con una serie de deficiencias que aún desisten de obtener el mismo nivel de protección con el que hoy en día cuenta España, tal es el caso de que "mientras que España es un Estado miembro de la Unión Europea, México es un tercer país que todavía no tiene nivel adecuado otorgado por la Comisión Europea"[97]. Así como que México es uno de los países con los niveles de sanciones más altos, más aún que España, "las sanciones en México, según lo previsto en la LFPDPPP, pueden sobrepasar el millón de euros"[98].

Por último, es importante hacer mención de todas las reformas a las que se está enfrentando España, para renovarse e incorporar su normatividad al reglamento de protección de datos que dispone la UE, todas las cuestiones de protección de datos que traen consigo las tecnologías así como las cuestiones de derecho de la información que España está comenzando a implementar a sus normatividades, es natural que México tampoco tiene en su reglamentación esas

[97] *Acuerdos comerciales entre la Unión Europea y Latinoamérica*, Valencia, Universidad Internacional de Valencia, 2015, p. 19.
[98] *Idem.*

cuestiones, por lo que, hoy en día se encuentra en una desventaja frente a los países que componen la UE y en especial frente a España, quienes ya están comenzando a implementarlo.

Es necesario que México comience a realizar de manera urgente una serie de reformas a su legislación para contemplar los temas de protección de datos que España comienza a implementar, puede ser una buena forma, tomar ventaja de ese termino con el que cuentan todos los países de dos años para adaptar su legislación, y así poder tener en un término equivalente las mismas formas de regulación y tratamiento de datos personales que la globalización actual exige.

2.4.2. En el ámbito internacional

Años posteriores a la llamada revolución tecnológica del siglo XX, la OCDE fue una de las primeras instituciones en crearse para proteger la privacidad de las personas, la participación entre los estados permitió que comenzara a protegerse el tema y la importancia de protección a nivel internacional, fue una manera efectiva de comenzar con un proyecto de protección, sin embargo, no fue el más efectivo.

En virtud de lo anterior, en año de 1981, “el Consejo de Europa adoptó el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, también conocido como "Convenio de Estrasburgo"[99]. Este convenio fue el primero en tomar de manera efectiva la forma de un acuerdo, y en él se contenían de manera específica cuestiones de protección de datos haciendo la distinción entre el sector público y el sector privado.

Al igual que la organización, el convenio fue adoptado por varios países, pero continuaba sin tener una aplicación eficaz en un número significativo de países, por lo que rápidamente fue perdiendo participación e importancia,

[99] *Idem*

simplemente se sabía que existía, pero no era tomado en cuenta para hacer efectivo su reglamentación.

No fue hasta el año de 1995, que la UE creó una directiva especial con aplicación obligatoria para todos los países que eran miembros directos y que la conformaban, y éste "establece un régimen normativo exhaustivo que reglamenta el tratamiento de los datos personales"[100]. A razonamiento de Cerda Silva "ella ha contribuido notablemente a la armonización entre los países miembros de la Unión Europea"[101], y efectivamente, con respecto a la regulación y protección de datos personales hoy en día Europa cuenta con una amplia protección de datos, esto ha sido reconocido a nivel mundial. "La Directiva 95/46/CE, fue adoptada en 1995 con un doble objetivo: defender el derecho fundamental a la protección de datos y garantizar la libre circulación de estos datos entre los Estados miembros"[102].

Así, la búsqueda de una nueva protección de los Estados con respecto al derecho a la intimidad de toda persona, es resultado de una necesidad actual que solo pudo visualizarse y comenzarse a regular a través del uso de un método científico para poder llegar a una solución concreta.

Por otro lado, tomando como ejemplo España, no fue sino hasta la década de los 90 que comenzaron a aparecer las primeras normativas que dieron pauta al inicio de regulación de temas de privacidad en la materia.

En España se realizó la aprobación en el año de 1992 la LORTAD, pero tal y como afirma Vera Santos, "hasta esa fecha la regulación al respecto, a partir del artículo 18.4 partía de la convención de 1981, sobre protección de las personas respecto al tratamiento automatizado de datos de carácter personal"[103].

Posteriormente se aprobó la Directiva 95/46/CE y se realizaron cambios considerables a la ley LORTAD, por lo que se decidió aprobar la ley que hasta la

---

[100] *Cerda Silva, Alberto, "El nivel adecuado de protección, para las transferencias internacionales de datos personales desde la Unión Europea", Revista de Derecho Valparaíso, núm. 36, p. 327*

[101] *Idem*

[102] Zeballos Emilia, *La protección de datos personales en España,* Madrid, tesis para obtener el grado de doctora, Universidad Complutense de Madrid, 2013, p. 25.

[103] Vera Santos, José Manuel, "Derechos fundamentales, internet y nuevas tecnologías de la información y de la comunicación", en García Mexia, Pablo (director), *Principios de derecho de internet*, 2a ed., Valencia, Tirant lo Blanch, 2005, p. 211.

fecha rige y protege lo concerniente al tratamiento de datos personales, la Ley Orgánica 15/1999 de protección de datos personales. Ésta fue reemplaza por la nueva normativa denominada Ley Orgánica de Protección de datos y Garantía de los Derechos Digitales (LOPD) 2018 la cual, a partir de noviembre de 2018, comenzó con aplicación absoluta en España con respecto a la protección de datos personales de carácter personal; y misma que fue publicada con fecha 30 de julio de 2018 y denominada por el gobierno español como el Real Decreto de Ley 5/2018, misma que fue remitida al Congreso de los Diputados para su respectiva sanción, esto para cubrir la imperante necesidad de adaptación del Estado Español de la nueva directiva europea en materia de protección de datos.

Por su parte, la UE está alineada en cuanto a protección de datos personales en el comercio electrónico se refiere, a través del RGPD.

Con lo que respecta a la aplicación directa de actividades que promuevan la protección de datos en el ámbito del comercio electrónico dentro de un país miembro de la UE, se puede afirmar que España es uno de los países miembros que ha tomado partido para su implementación y diseño de actividades que promuevan su utilización y debido cumplimiento.

España a través de la AEPD, ha diseñado una herramienta online que permite que pequeñas y medianas empresas que participen en actividades mercantiles y que como producto de esas actividades recaben información que se considere de bajo riesgo para los derechos y libertades de sus ciudadanos, puedan tener un apoyo directo del gobierno para cumplir con la normatividad vigente en materia de protección de datos.

La herramienta en línea diseñada por la AEPD se denomina “Facilita”[104]. Esta herramienta proporcionada de forma gratuita y de fácil acceso a través de la plataforma de la Agencia Española cuestiones básicas que permitirán alinearse de manera sencilla, a los estándares mínimos establecidos por el Reglamento de Protección de Datos Personales, lo único que la propia agencia específica para

[104] Herramienta en línea enfocada en ayudar a empresas al tratamiento de datos personales considerados de bajo riesgo, para estar en optimas condiciones de cumplir con el nuevo Reglamento de Protección de Datos Personales de la UE, https://www.aepd.es/herramientas/facilita.html.

que pueda ser posible estar en armonía con la herramienta en línea y con la propia Ley, es no ser una empresa que trate datos personales y que estos mismos datos sean considerados de alto riesgo para los derechos y libertades de las personas.

Es importante recalcar que esta herramienta solo será aplicable a aquellas empresas que traten datos que se consideren de escaso riesgo, por lo que en un inicio, deberá de responderse a una pequeña encuesta que tendrá como finalidad determinar aquellas actividades que se constituyan alto riesgo para el tratamiento de datos personales.

Las actividades que son consideradas de alto riesgo y que por ende no podrán ser apoyados por parte de la AEPD son los siguientes:

- Sanidad.
- Solvencia patrimonial y de crédito.
- Generación de uso y perfiles.
- Actividades políticas, sindicales, religiosas.
- Servicios de Telecomunicaciones
- Seguros.
- Entidades bancarias y financieras.
- Actividades de servicios sociales.
- Publicidad.
- Video vigilancia masiva, (video vigilancia de grandes infraestructuras como estaciones de ferrocarril o centros comerciales).

En el supuesto de que una de las anteriores actividades sea materia de comercio electrónico de alguna empresa, no podrá utilizar el servicio de “Facilita” y por ende deberá de realizarse un análisis de riesgos, el cual señala el mismo RGPD.

Si se cuenta con un *e-commerce* que no corresponda con la lista anterior y por ende, no trate datos considerados de alto riesgo, la herramienta en línea, podrá ser de mucha ayuda para generar de manera automática varios documentos

que serán de gran utilidad para que la empresa cumpla con la normatividad en temas de protección de datos personales, adecuándose al RGPD.

Entre los documentos que emite la herramienta en línea son:

- Clausulas informativas que permitan la recogida de datos personales.
- Cláusulas contractuales para anexar a los contratos de encargados del tratamiento.
- Anexos que contengan medidas de seguridad mínimas para el correcto tratamiento de los datos personales.

Es importante considerar que la herramienta que ofrece el gobierno español, es únicamente de ayuda, por lo que en todos los casos deberá de verificarse y adaptarse a los casos concretos, para que tenga un diseño completamente adaptado a la empresa o negocio.

Otro de los aspectos que implementó la AEPD es una guía que especifica la directrices que deben de contener los contratos que se celebren entre los responsables y los encargados de la información, y en donde se estipularán los mínimos legales que señala el RGPD. El acuerdo deberá de contener como mínimo:

a) La forma en que el responsable de la información deberá de tratar los datos personales: En dicho sentido, deberá de especificarse de forma clara la forma en que debe de tratarse los datos recabados, en función del servicio que se va a prestar y la forma en que será prestado, y especificar que dichas obligaciones serán transferidas en su totalidad cuándo exista un encargado.
b) Protección del derecho de confidencialidad: El contrato deberá de señalar de forma clara, concisa y expresa la obligación del encargado de garantizar que la información será en todo momento tratada de manera confidencial y que únicamente las personas autorizadas para conocerlas podrán acceder a la información, garantizando previamente el mismo nivel de confidencialidad al que fue comprometido.

c) Las medidas de seguridad a implementar: el contrato deberá de establecer de manera clara las medidas de seguridad a los que el responsable y el encargado deben de comprometerse, siempre actuando de conformidad con lo que estipula el RGPD.
d) El régimen de subcontratación: Deberá estipularse en el contrato que se tiene con la autorización previa por escrito antes de que el encargado subcontrate los servicios, y en tal situación, el sujeto que sea subcontratado tendrá la obligación de cumplir cabalmente con todas las obligaciones a las que el encargado se obligó inicialmente.

Los derechos de los titulares de la información: El contrato deberá de establecer de forma clara cómo será la asistencia de los titulares de la información por parte de los encargados, así como de los derechos que les asisten; incluyendo de manera general el derecho de acceso, rectificación, supresión, limitación, portabilidad y el derecho a oposición.

Es menester considerar que la protección de datos se materializa en el momento en que los sujetos encargados de la protección de información hacen adecuaciones considerables en los sistemas de protección de información que emplean para que los datos no se encuentren vulnerados y en el plano internacional, Latinoamérica ha contribuido a adoptar sistemas internacionales para que este tipo de controles de seguridad sean posibles.

Uno de los países latinoamericanos que ha desarrollado grandes proyectos en el sector empresarial para la protección de información es Ecuador; quién ha llamado la atención, tanto de empresas ecuatorianas como del gobierno de Ecuador, precisamente por la forma en que ha regulado la protección de información y por las políticas internacionales que ha implementado para asegurar forma en la que debe de protegerse la misma.

Para Proaño Escalante y Gavilanes Molina, “Garantizar la seguridad de la información, los sistemas de información, servicios y redes implica socializar, también conocer cómo responder ante un evento donde se ha vulnerado dicha seguridad informática y cómo gestionar la evidencia digital identificada,

fruto de una vulnerabilidad de seguridad informática"[105]. Es decir, no es necesario el contar con la mayor cantidad de medidas de seguridad que las tecnologías de la información ofrezcan, es necesario que las empresas cuenten además con una serie de políticas mínimas que como organización les permitan conocer la forma en que deberán de actuar en caso de alguna vulneración en sus sistemas informáticos. Se ha llegado a señalar lo siguiente:

> Los incidentes de seguridad informáticos y ciber delitos se generan, entre otras causas, por una deficiente cultura digital y moral, además de una carente o por lo menos deficiente normativa respecto a la manipulación, transmisión, recuperación y almacenamiento de los datos y evidencias. El desconocimiento u omisión de buenas prácticas incrementa las vulnerabilidades de seguridad[106] .

Lo primero que Ecuador investigó como país, fue la identificación de deficiencias en el área de la información y la forma en la que debía proteger esa información, así como la comparativa desde el punto de vista jurídico, con respecto a otros países. De entre algunas de las deficiencias que Ecuador identificó con respecto a las normatividad referente a la protección de información, se encuentran las siguientes causas:

1. Que no existan profesionales debidamente capacitados para atender gestiones directamente relacionadas con los indicios digitales, es decir, que den un correcto seguimiento a los principales delitos cuando estos se den a través de medios digitales, tal es el caso del robo, fraude, sabotaje, etc. Los cuales en la mayoría de las ocasiones quedan impunes porque no se les da un adecuado seguimiento.
2. No está reconocida la figura del Perito informático en la legislación ecuatoriana, toda vez, que el código penal de ese país no ha establecido un modelo unificado que contemple y regule su ejercicio, lo cual ha ocasionado que los delitos que se den a través de medios digitales, no puedan ser

[105] Proaño, Escalante, Rodrigo y Gavilanes, Molina, Andrés, "Estrategia para responder a incidentes de inseguridad informática ambientado en la legalidad ecuatoriana", *Enfoque UTE*, Marzo 2018, p.90, *http://ingenieria.ute.edu.ec/enfoqueute/*
[106] *Ibidem*, p.91

perseguidos e investigados adecuadamente, debido a la falta de especialización para su indagación[107].

3. Si bien es cierto, la normatividad ecuatoriana en su servicio ecuatoriano de normalización, se ha señalado que "la reglamentación técnica comprende la elaboración, adopción y aplicación de reglamentos técnicos necesarios para precautelar los objetivos relacionados con la seguridad, la salud de la vida humana, animal, vegetal, la preservación del ambiente y la protección del consumidor contra prácticas engañosas"[108], no se han creado estudios serios sobre la reglamentación de prácticas derivadas de los medios tecnológicos.

Una vez identificado lo anterior, Ecuador se dio a la tarea de realizar una investigación de normatividad internacional y conocer el panorama que tenían otros países con respecto a la protección de información, logrando proponer puntos clave de gestión de información. A través de propuestas, la sociedad ecuatoriana sugirió comenzar a atacar el problema de inseguridad en la información, proponiendo la creación de guías de protección, recolección, tratamiento y extracción de información, utilizando de base algunas normatividades que se utilizan en el plano internacional, tales son el caso de:

- **ISO/IEC 27000.** Sistemas de gestión de la seguridad de la información, resumen y vocabulario (*Information security management systems Overview* and *vocabulary*, denominación en inglés),
- **ISO/IEC 27037.** Directrices para la identificación, recolección, adquisición y preservación de la evidencia digital (Guidelines for identification, collection, acquisition and preservation of digital evidence, por denominación en inglés).

A continuación me permito realizar una pequeña introducción de la normatividad ISO/IEC27000.

[107] *Idem*
[108] *Idem*

La ISO/IEC 27000.- Ésta ha sido catalogada como la normatividad de protección de información más importante hasta el momento, toda vez que engloba una serie de normativas enmarcadas exclusivamente a la protección de la información.

> la serie ISO/IEC 27000 publicadas por la ISO y la Comisión Electrotécnica Internacional (IEC), compuesta por aproximadamente 17 normas, clasificadas en cuatro categorías: *i*) La norma que contiene el vocabulario, contenido en la norma ISO/IEC 27000; *ii*) las normas de requerimientos, contenidos en la norma ISO/IEC 27001 y la norma ISO/IEC 27006; *iii*) las normas guía desarrolladas a través de 10 normas: ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27007, TR 27008, ISO/IEC 27013, ISO/IEC 27014, TR 27016, ISO/IEC 27032 y *iv*) las normas para sectores específicos, contenidas en las normas ISO/IEC 27010, ISO/IEC 27011, TR 27015 y TS 27017[109]

Aunque se pueden identificar una cantidad considerable de normas de la serie 27000, existen cuatro tipos de normatividades que están enfocados exclusivamente a la forma en que una empresa u organización debe de estar conformada para tener un adecuado nivel de protección de información.

Norma ISO/IEC 27001.-La cual es conocida como *Tecnología de información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información – Requerimientos.* Ésta se encuentra elaborada para señalar los requisitos necesarios para implementar, operar, monitorear, revisar y mantener en constante mantenimiento el Sistema de Gestión de información. Se ha considerado como la más importante para poder obtener la certificación de la normatividad ISO 27001.

Esta normativa se encarga entre otras cosas de mantener los sistemas de gestión de información en evaluación constante para que se identifiquen los riesgos y amenazas que puedan poner en peligro inminente la información de una empresa o de los terceros. Esta normativa tiene la importancia de estar enfocada en la información de la empresa y se encuentra íntimamente ligada con otras dos normas ISO: la ISO 22301 de continuidad del negocio y la ISO/IEC 20000 de gestión de servicios TI[110]

[109] Valencia Duque, Francisco Javier y Orozco Álzate, Mauricio, *op, cit*.
[110] La norma ISO 27001: Aspectos claves de su diseño e implantación, *www.isotool.org*

Por una parte la norma ISO 22301 contribuye a reforzar la normativa 27001 porque cuenta con el sistema de tiempos de recuperación que permite evaluar planes de contingencia y una vez superada reanudar la actividad de manera inmediata, por su parte la norma ISO 20000 contribuye a gestionar la calidad que ofrecen los servicios de TI, tal es el caso de las páginas web, *hostin, elearning*[111].

Norma ISO/IEC 27002.- La cual es conocida como *Tecnología de información - Técnica de seguridad - Código de prácticas para controles de seguridad de la información.* Ésta norma sirve de base para ayudar a las empresas a crear sus propias normatividades de protección de información, sirve para seleccionar controles de acceso de procesos e implementación de controles de calidad.

Norma ISO/IEC 27003.- Ésta normatividad es llamada *Tecnología de información - Técnica de seguridad - Guía de implementación de un sistema de gestión de seguridad de la información,* la cual ayuda a realización de una propuesta metodológica de especificaciones y diseño de un sistema de seguridad.

Norma ISO/IEC 27005.- Denominada *Tecnología de la información - Técnicas de seguridad - Gestión del riesgo en la seguridad de la información*, ayuda a crear proyectos de gestión de riesgos dentro de la implementación de sistemas de seguridad[112].

Se considera que para que las empresas puedan contar con un adecuado sistema de gestión y protección de información, es necesario que se certifiquen en normativas previas especializadas en la materia. Deberán de aprovechar de éste de regulaciones internacionales, toda vez que se permitirá comprobar a otra empresa, que cuenta con sistemas previamente establecidos, hasta llega estar en un mismo nivel de protección de otros países del mundo, por lo que traerá consigo la confianza de participación internacional en materia de comercio.

[111] *Idem*
[112] Valencia Duque, Francisco Javier y Orozco Álzate, Mauricio, *op, cit*.

2.5. Elementos comparativos a la normativa jurídica del derecho derivados del e-commerce en México y la Unión Europea

La relación económica derivada del comercio electrónico entre México y Europa ha despegado a partir de la cooperación internacional en la que han participado ambas naciones para poder llevar a cabo una actividad colaborativa legalmente reconocida. El TLCUEM ha sido uno de los principales ordenamientos internacionales que ha fortalecido y reconocido desde el ámbito internacional, dicha situación.

El TLCUEM se encuentra en vigor para aplicación entre ambas naciones a partir del año 2000 y fue resultado de una serie de acuerdo en los que intervino la Asociación Económica, Concertación Política y Cooperación México-UE y que buscaban una finalidad común, fomentar la cooperación y el dialogo[113]. Es menester mencionar que México fue el primer país en Latinoamérica en llevar a cabo la celebración de un tratado de esta naturaleza.

El tratado señalado con antelación ha permitido que entre ambas naciones se lleven a cabo una serie de leyes y normativas que permiten la cooperación mutua internacional para llevar a cabo de manera diplomática y accesible las importaciones provenientes de la UE hacia México y por otro lado las exportaciones de México hacía la UE.

Posteriormente, en el mes de abril del 2018 se llevó a cabo el proceso de negociación y modernización del acuerdo Global México- La UE, el cual incluye principalmente la renegociación de aspectos políticos, económicos y de cooperación, “logrando concluir los capítulos en materia de obstáculos técnicos al comercio; empresas propiedad del Estado; subsidios; comercio de servicios en lo relativo a reglamentación nacional, telecomunicaciones, transporte marítimo y servicios de entrega; y anticorrupción”[114].

---

[113] TLC México- Unión Europea, Subsecretaría de Comercio Exterior, Secretaría de Economía, *http://www.bruselas.economia.gob.mx/swb/swb/bruselas/TLC_Mex_UE*

[114] Centro de Estudios Internacionales Gilberto Bosques, "Principales aspectos del nuevo Tratado de Libre Comercio entre México y la Unión Europea (TLCUEM): oportunidades, logros y desafíos", Nota de Coyuntura, México, Senado de la República, 3 de mayo de 2018.

De igual manera “Cabe mencionar que el Tratado amplía también la cobertura en el comercio de servicios, ya que contempla un apartado de telecomunicaciones y la entrada temporal de personas y servicios relacionados con la economía digital”[115], es decir, con esta inclusión se reconocen los diferentes medios tecnológicos y de comunicación para llevar a cabo un comercio trasnacional, tal es el caso del *e-commerce*, donde se estipulan las directrices para su reconocimiento y regulación, acordando que no impondrán aranceles especiales por comerciar productos o servicios a través de trasmisiones electrónicas y logrando así facilitar la provisión de los productos y/o servicios.

Es importante señalar que aunque el principal objetivo de este tipo de normativa entre ambas naciones tienen es marcar las directrices de comunicación y regulación para llevar a cabo un comercio internacional eficaz y coordinado, el tema de la protección de información, como se ha observado en los capítulos precedentes y como podrá apreciarse en los capítulos posteriores será regido de acuerdo a los estándares de seguridad de cada una de las naciones establece para proteger su información de carácter personal y sobre todo se ceñirán de acuerdo a lo que en este marco bilateral, en concreto conformado por la UE y México, establece para proteger la información de carácter personal que derivado del *e-commerce* trasnacional pudieran compartir.

[115] *Idem*

CAPÍTULO 3
EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS PERSONALES DE LA UNIÓN EUROPEA

SUMARIO: *3.1. Proceso histórico de adaptación del Reglamento General de Protección de Datos de la Unión Europea; 3.2.Análisis de principales normatividades de protección de información para el comercio electrónico; 3.3. Análisis de principales derechos inherentes a las tecnologías de la información en materia de protección de datos personales para el comercio electrónico contenidos en el RGPD; 3.4. Ejercicio comparativo de normativas legales en materia de protección de datos para el e-commerce: RGPD y LFPDPPP*

En el presente capitulo podrá apreciarse la presencia que tiene el RGPD en la UE; así mismo, se identificarán las principales disposiciones que emanan de la normativa y las novedades que para el comercio electrónico han implementado.

3.1. Proceso histórico de adaptación del Reglamento General de Protección de Datos de la Unión Europea

El Reglamento de la UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (RGPD) es uno de los proyectos más completos hasta la fecha en temas de protección de información y uno de los proyectos más ambiciosos que ha tenido la Unión Europea para enfrentar los cambios digitales y tratar de tener un ambiente armonizador en materia de protección de datos personales.

Fueron más de 4 años el proceso que llevó la elaboración y aprobación del proyecto, que finalmente en Bruselas se publicó el día 27 de abril de 2016 y en el que, todos los países integrantes de la UE, se adherían automáticamente a él por pertenecer a dicha comunidad.

El proyecto del RGPD fue presentado el día 25 de enero de 2012, posteriormente fue discutida durante el año 2015 por parte del Parlamento Europeo, el Consejo y la propia Comisión Europea, y fue hasta abril del siguiente año, cuando se aprobó por parte del Consejo de la UE; sin embargo ésta no fue la definitiva, toda vez que Austria pronunció la baja protección que el reglamento ofrecía en comparación con la directiva vigente hasta ese momento, la directiva 95/46/CE[116], no fue sino hasta el día 27 de abril de 2016 que finalmente fue aprobada por el Parlamento Europeo. Su publicación en el Diario Oficial de la UE, se dio a conocer el día 04 de mayo de 2016, entrando en vigor dentro de los veinte días posteriores; por último, tomando en cuenta las cantidad significativa de cambios que constituía el reglamento, se le extendió un plazo de dos años para que todos los sujetos a los que impactará directamente su contenido, tuvieran oportunidad de realizar las medidas y cambios oportunos a sus organizaciones para el debido cumplimiento, en virtud de lo anterior, el reglamento es de aplicación absoluta a partir del día 25 de mayo de 2018, fecha en la cual ya se cuentan con todas las facultades para poder exigir su aplicación absoluta.

El RGPD ha sido uno de los proyectos más ambiciosos que ha tenido la UE para enfrentar los cambios digitales y tratar de tener un ambiente armonizador entre países, para que pueda ser un derecho reconocido y observado desde un punto más acercado a lo que la globalización necesita hoy en día.

Es importante considerar que el RGPD, tuvo como base para elaboración, diversas problemáticas previas que sus Estados miembros experimentaron durante su negociación y redacción, existen sentencias relevantes que dieron lugar a nutrir las necesidades que experimentaba la UE para armonizar un derecho común y de protección para sus ciudadanos, se consideran dichas apreciaciones en sentencias como:

a) La Sentencia del Tribunal de Justicia a través de la Gran Sala, de fecha de 8 de abril de 2014 relativa a Comunicaciones electrónicas, La Directiva 2006/24/CE enfocada a Servicios de comunicaciones

[116] Vote watch Europe, *https://www.votewatch.eu/en/term8-regulation-of-the-european-parliament-and-of-the-council-on-the-protection-of-natural-persons-with-r.html*

electrónicas de acceso público o de redes públicas de comunicaciones y con respecto a la Conservación de datos generados o tratados en relación con la prestación de tales servicios, revisando la validez de los artículos 7º, 8º y 11º de la Carta de los Derechos Fundamentales de la UE (Caso Digital Rights Ireland,Ltd)

b) SENTENCIA DEL TRIBUNAL DE JUSTICIA a través de la Sala Tercera de fecha de 1 de octubre de 2015 relativa al procedimiento prejudicial, se realizó el análisis de la Protección de las personas físicas en lo que respecta al tratamiento de datos personales, estudiando a la Directiva 95/46/CE dentro de sus artículos 4º, apartado 1, y 28, apartados 1, 3 y 6, sobre el Responsable del tratamiento establecido formalmente en un Estado miembro, así mismo se estudió la vulneración del derecho a la protección de los datos personales relativos a las personas físicas en otro Estado miembro y la determinación del Derecho aplicable y de la autoridad de control competente, así como el ejercicio de las facultades de la autoridad de control y la Potestad sancionadora (Caso Weltimmo S.R.O.)

c) SENTENCIA DEL TRIBUNAL DE JUSTICIA de la Gran Sala, de fecha de 6 de octubre de 2015, relativa al Procedimiento prejudicial, Datos personales , Protección de las personas físicas frente al tratamiento de esos datos y la Carta de los Derechos Fundamentales de la UE, en sus artículos 7º, 8º y 47, así como a la Directiva 95/46/CE en sus artículos 25 y 28 relativos a la transferencia de datos personales a países terceros Facultades de las autoridades nacionales de control (Caso Schrems).

Las sentencias señaladas con antelación han contribuido considerablemente al texto actual del RGPD, toda vez que trataron temas con relación a la evaluación del impacto de la protección de información, la falta de protección de datos por parte de empresas no pertenecientes a la UE y las facultades de una autoridad de control competente, entre otros temas.

Así mismo, durante la evaluación de la Estrategia Europa 2020, donde se realiza la evaluación de instrumentos de la UE en materia de protección de datos, se llevó a cabo la realización de consultas entre los países de la UE, donde se concluyó que la principal preocupación de los grandes operadores de información, era la transferencia de datos hacia el exterior, y que la diversidad de normas que existían en cada unos de los países miembros, dificultaba considerablemente un adecuado tratamiento, por lo que se repercutía negativamente al desarrollo de empresas y del comercio, por lo que consideraban necesario la regulación y adopción de normas más adecuadas para armonizar la relación entre países y contribuir a la efectividad de su cumplimiento[117].

De acuerdo con lo señalado por Fuensanta Martínez el RGPD supera considerablemente la antigua directiva 95/46/CE y establece una serie de elementos y derechos que hasta el momento no se habían considerado en alguna otra legislación, se le da prioridad a los llamados derechos digitales, aumentando la seguridad jurídica de todo ciudadano miembro de la UE, toda vez que se le garantiza al máximo de una forma completamente estricta la protección de los datos personales[118].

Consecuencia de lo anterior, es importante recalcar que mientras la directiva 95/46/CE basaba su texto principalmente en el procedimiento que debían de llevar los responsables de los ficheros de datos, el RGPD, aunque es considerado un texto con mayores dificultades de interpretación y lectura, ayuda a establecer los retos en que las empresas deberán de comenzar a plantearse para realizar un correcto cumplimiento, es decir, se apuesta más por establecer los lineamientos para que las empresas comiencen a proteger adecuadamente los datos.

Tal y como lo marca el propio RGPD en su considerando 9º, “aunque los objetivos y principios de la Directiva 95/46/CE siguen siendo válidos, ello no ha

---

[117] Katarzyna Golinska, Mónica*, La evolución normativa del Derecho a la Protección de Datos*, Alcalá de Henares, Universidad de Alcalá, 2018, p. 24.

[118] Fuensanta Martínez, Martínez, Dolores, “Unificación de la protección de datos personales en la Unión Europea: desafíos e implicaciones”, *El profesional de la información*, España, 2018, núm. 1, p. 189.

impedido que la protección de los datos en el territorio de la Unión Europea se aplique de manera fragmentada… en relación con las actividades en línea"; desde el punto de vista del reglamento, las diferencias del nivel de protección de los datos personales de las personas físicas para poder asegurar sus derechos y libertades, se convierten en un obstáculo para que las actividades económicas a través de la UE y fuera de ella, se puedan cumplir adecuadamente[119].

El RGPD está conformado por noventa y nueve artículos y ciento setenta y tres consideraciones, los cuales abordan de manera general temas como el flujo transfronterizo de datos, datos genéticos y de salud, protección de datos de los niños, portabilidad de datos, transferencia a terceros y sanciones hacía los sujetos que estén obligados a su observancia y cumplimiento y no sean protegidos correctamente.

3.2. Análisis de principales normatividades de protección de información para el comercio electrónico

Una vez que comenzó a entrar el vigor el RGPD, es claro que la UE comenzó a ser más cuidadoso con la información que entra y sale de su territorio; y a su vez, que comenzara a ser más drástico en cuanto a sus decisiones, por un lado, para hacer valer la normativa y por el otro, de sancionar cualquier incumplimiento que se genere durante su vigencia.

En principio, es importante mencionar que el RGPD no tiene como finalidad el tratamiento de carácter personal de una persona física, cuando ésta proporcione sus datos para actividades exclusivamente relacionadas con actividades personales o domésticas, en virtud de lo anterior, deberán de tener conexión directa con alguna actividad profesional o comercial. Así mismo, el citado reglamento es extensible para los responsables y encargados de proteger los datos personales, cuándo estas obligaciones deriven de alguna actividad profesional y/o comercial, pero como excepción también para aquellos que

[119] De acuerdo con el considerando número 9º del Reglamento de la Unión Europea (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

proporcionen los medios para tratar los datos personales relacionados con las actividades personales y domésticas.

El comercio electrónico será uno de los principales sectores que comenzarán a ser flanco de observancias para corroborar que efectivamente se está aplicando de manera adecuada el Reglamento, toda vez que éste será directamente aplicable a empresas, entidades y organizaciones que tengan en común la finalidad de comercio electrónico y que para ese fin tengan la obligación el tratamiento de datos de carácter personal.

De primer momento, es conocido que el principal motor de funcionamiento del comercio electrónico son los datos, es decir, todas las transacciones que se realizan, la información que se intercambia, los productos o servicios que se ofrecen y los acuerdos de voluntades que perfeccionan un contrato de compra-venta, en el caso del *e-commerce*, se realizan por medio de datos; por lo que, para estar en completo cumplimiento de la ley, debe de cumplirse a cabalidad lo señalado por el RGPD. Se considera que si el comercio electrónico con lo que respecta a España, se adapta a lo establecido en el RGPD y la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, tendrá gran avance en el cumplimiento de sus principales obligaciones como prestadores de productos y servicios, toda vez que garantizará ante la Ley, la protección de la privacidad y derechos de los usuarios.

La reforma en materia de protección de datos que muestra el RGPD tiene unos objetivos precisos y hasta cierto punto considerados como drásticos; tal y como señala la autora Fuensanta "se abandonan los instrumentos armonizadores en favor de los unificadores como el reglamento comunitario, apostando por el fomento de las TICs como una política europea horizontal que afecta a todos los sectores económicos y al sector público"[120]. Por lo anterior, España ha trabajado en base a lo estipulado en el Reglamento en los siguientes derechos, señalando de manera particular los siguientes:

[120] Fuensanta, Martínez, Martínez, Dolores, "Unificación de la protección de datos personales en la Unión Europea: desafíos e implicaciones", *El profesional de la información*, Murcia, vol.27, núm.1, pp. 185-194.

3.2.1. Evaluación y control de riesgos de la información

Para que pueda llevarse a cabo una correcta aplicación de la protección de datos en el *e-commerce*, es necesario que los prestadores de productos o servicios garanticen un correcto tratamiento de datos personales de las personas con las que realizarán operaciones mercantiles a través de medios electrónicos o las tecnologías de la información. Para que lo anterior tenga una completa aplicación y eficacia, es necesario que primeramente, cada uno de los responsables que dispongan de un *e-commerce*, realicen una auditoria para identificar qué datos hasta el momento están tratando y para qué finalidades; y una vez hecho lo anterior, puedan decidir qué tipo de adecuaciones realizar y qué infraestructura es necesaria implementar para poder estar en completo cumplimiento de su legislación nacional e internacional a la que se encuentran obligados por pertenecer a la UE.

El punto anterior está respaldado mediante el Reglamento de la UE 2016/679 a través de su artículo 35 el cual establece que es necesaria la evaluación del impacto relativa a la protección de datos. El propio inciso 1 del artículo 35 lo enuncia de la forma siguiente:

> Cuando sea probable que un tipo de tratamiento, en particular si utilizan las tecnologías de la información y comunicaciones, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares[121].

Lo anterior reafirma que es necesario que de ahora en adelante el responsable de la información cuando se trate de alguna actividad como el *e-commerce,* la cual funciona prácticamente de la utilización de las tecnologías, debe de realizar a través de un asesoramiento debido, como puede ser por medio de un delegado de protección de datos o de alguna institución especializada en el tema, para medir la situación actual en la que como empresa se encuentra, o

[121] Artículo 35 del Reglamento de la UE 2016/679 del Parlamento Europeo y del Consejo.

evaluar el posible riesgo que puede considerarse por la utilización de datos personales.

Con lo que respecta a la ley española, la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, no contempla directamente esta obligación para el *e-commerce*, es decir, solo se establece en su disposición adicional decimoséptima correspondiente al tratamiento de datos de salud, que esta obligación sólo podrá tener lugar cuándo de acuerdo a lo previsto en el artículo 89 del Reglamento de la UE 2016/679 se "lleve a cabo un tratamiento con fines de investigación en la salud pública, y en particular biomédica"[122].

De lo anterior, podría inferirse que la principal preocupación de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de España, únicamente ponen principal interés en temas considerados como de vanguardia, es importante mencionar que el comercio electrónico ya tiene varios años con legislación propia dentro de la UE, sin embargo, se considera imprescindible el reconocimiento en esta misma ley de lo correspondiente al *e-commerce,* solo así podrá observarse un cumplimiento puntual este tema en particular.

3.2.2. El delegado de protección de datos personales

Un delegado de protección de datos es aquella persona encargada de informar y asesorar de manera frecuente al responsable del tratamiento de la información, así como a los encargados y a los empleados de éste último que a su vez se encuentren a cargo del tratamiento de datos, en especial sobre las obligaciones que derivan directamente del cumplimiento de lo establecido en el RGPD, así

[122] Párrafo 1º inciso f) de la "Disposición adicional decimoséptima (nueva). Tratamientos de datos de salud", *Proyecto de Ley Orgánica De Protección De Datos Personales y Garantía De Los Derechos Digitales (Antes denominado proyecto de ley orgánica de protección de datos de carácter personal*, Congreso de los Diputados, 17 de octubre de 2018, Serie A, núm. 13-4, p. 54.

mismo serán encargados de supervisar que se cumplan todas y cada una de las disposiciones de protección de datos de la UE y de los Estados miembros[123].

La figura del DPO, será imprescindible para llevar a cabo el correcto tratamiento de datos, para aquellas empresas o instituciones que manejen una cantidad considerable de datos, las empresas dedicadas al *e-commerce* serán algunas de ellas.

Entre las principales funciones que tendrán a su cargo los delegados de protección de datos, de acuerdo con lo establecido en el artículo 39 del RGPD, se encuentran los siguientes:

1. Informar y asesorar al responsable, encargado y empleados de estos sobre las principales responsabilidades en materia de protección de datos personales e interpretación del RGPD.
2. Supervisión del debido cumplimiento del RGPD, concienciación, formación y asignación de responsabilidades al personal que lo requiera.
3. Asesorías acerca de la evaluación del impacto que en materia de riesgos especifica el artículo 35 del RGPD.
4. Cooperar con la autoridad de control.
5. Ser un punto de contacto entre la autoridad de control y el responsable y encargado de los datos personales.

Por su parte la legislación española a través de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, establece en su artículo 34 la delimitación de los supuestos en lo deberá de designarse de manera específica un delegado de protección de datos, contemplando de manera específica a los supuestos relacionados con el *e-commerce*, tal y como a la letra se señala en el artículo 34 de la citada Ley:

> c) Las entidades que exploten redes y presten servicios de comunicaciones electrónicas conforme a lo dispuesto en **su legislación específica**, cuando traten habitual y sistemáticamente datos personales a gran escala.
>
> d) Los prestadores de servicios de la sociedad de la información cuando elaboren a gran escala perfiles de los usuarios del servicio.

[123] Artículo 39 del Reglamento de la Unión Europea (UE) 2016/679.

La Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales también retoma las principales cualidades del delegado de datos, de acuerdo con su artículo 35 deberá de acreditar su capacidad para ejercer el cargo, con la acreditación de los estudios debidos en materia de derecho y conocimientos en la práctica de la protección de datos. Asimismo, se le faculta a los delegados para que, de acuerdo al artículo 36 de la Ley, pueda observar los procedimientos relacionados con la propia Ley y emitir recomendaciones en el ámbito de su competencia, por último se agrega la independencia del delegado de protección de datos dentro de la organización, debiendo evitarse cualquier conflicto de intereses.

Tal y como puede observarse con lo mencionado anteriormente y en apoyo a lo manifestado el autor Martínez, Martínez, "el Reglamento General de Protección de Datos, no es una norma que admita aproximaciones de sillón, obliga al jurista a trabajar a pie de obra, a ensuciarse las manos en procesos que implican una profunda transformación organizativa y técnica"[124]

Sin embargo, se considera que se le debe dar un crédito importante al nuevo RGPD, como un avance significativo en temas de protección de información, a decir verdad, el que las empresas dedicadas al comercio electrónico, antes de la entrada en vigor del Reglamento supieran como establecer prácticas para que la información de sus usuarios fuera benéfica para otras prácticas comerciales no autorizadas, dejaba sin control de la información a los propios usuarios, de ahora en adelante, las formas de recolección y tratamiento de información serán completamente diferentes.

La transformación digital debe ser un proceso regido por el Derecho. En el anterior epígrafe se señalaron distintas normas que han ido incidiendo profundamente en esta materia desde diversos ámbitos. La tecnología debe tener en cuenta el ineludible valor que representa la dignidad humana y el respeto de los derechos fundamentales. En este sentido, en demasiadas ocasiones se nos dice

[124] Martínez Martínez, Ricard, "transformación digital y diseño orientado a la privacidad en la Universidad" *RUIDERAe: Revista de Unidades de Información*, Valencia, UCLM, 1er semestre 2018, núm. 13, p.2.

que “no cabe poner puertas al campo, o que el legislador siempre va por detrás de la tecnología. Estos argumentos han sustentado en más de una ocasión una suerte de falacia de la inevitabilidad tecnológica, a la que se une otra, que vendría a afirmar que el Derecho opera como un freno a la ciencia y a la innovación”[125].

Por ello, parece plenamente justificada la apuesta de la UE por una garantía fuerte del derecho fundamental a la protección de datos mediante una norma que regula los procesos de tratamiento de la información desde su diseño hasta su final, insertando en su ADN el respeto de los derechos fundamentales[126].

Se trata además de un sistema que refuerza su modelo de garantías mediante las autoridades de protección de datos a las que confiere elevados poderes de *enforcement*, y un marco sancionador altamente exigente[127].

Si deja de considerarse al RGPD como una normativa a la que hay que cumplir, y se comienza a observar su objetivo como una directriz para los responsables de la información, se podrá realizar, tal y como el mismo Reglamento lo señala en su considerando número 12, “contribuir al correcto funcionamiento del mercado interior garantizando la libre circulación de los servicios”

3.3. Análisis de principales derechos inherentes a las tecnologías de la información en materia de protección de datos personales para el comercio electrónico contenidos en el Reglamento General de Protección de Datos

El RGPD está conformado por varios principios que tienen como objetivo principal proteger la información relativa a una persona física identificada o identificable, para que pueda considerarse que cuenta con la denominación de identificada o identificable, deberá primero realizarse el cuestionamiento de si el responsable que cuente con la información puede a través cualquier medio que le permita singularizar a esa persona, llegar a conocer que existe grandes posibilidades de que se pueda inferir que se trata exclusivamente de esa persona.

[125] *Ibidem,* p.11.
[126] *Ibidem*, p.13.
[127] *Idem.*

Por lo anterior, es importante señalar que el RGPD, de primer momento establece que será únicamente aplicable para aquellos datos de personas físicas que puedan ser identificadas y/o identificables, por lo que excluirá de manera definitiva a toda aquella información que sea considerada como anónima, es decir, que no exista forma de que a través de mecanismos físicos o electrónicos, se pueda conocer a quién pertenece esa información.

Lo anterior nos hace reflexionar y darnos cuenta de primer momento que es necesario comenzar a desterrar una concepción formal de la protección de los datos personales. Considerando lo afirmado por Martínez, Martínez, no es intención principal únicamente proteger datos, toda vez que no debe de entenderse como una aplicación lo que parece concebirse por algunos como una burocracia insufrible. La finalidad es proteger personas y por consiguiente garantizar sus derechos, "aseguramos el pleno desarrollo de su personalidad en el contexto de una transformación digital acelerada[128]

El RGPD contiene principios nucleares que ayudan a conocer el alcance de las finalidades que persigue conseguir, así como la forma en la que se puede cumplir adecuadamente con su cumplimiento, estos principios, son conocidos dentro de la normativa específicamente en su artículo 5, los cuales me permito explicar en líneas subsecuentes:

a) Principio de licitud.- Toda la información personal deberá de utilizarse únicamente para tratar actividades u objetivos que sean lícitos dentro de los ámbitos y normativas comerciales, no se considerarán para la publicidad engañosa o para actividades que sean consideradas como ilegales.

   El principio de licitud es extensible y señalado en el artículo 6 del Reglamento, en el cual se señalan específicamente cuando será considerado licito el tratamiento de los datos:

   i. Cuando el interesado dio su consentimiento
   ii. El tratamiento es indispensable para la ejecución de un contrato
   iii. Para el cumplimiento de una obligación legal

[128] *Ibidem*, p.13.

iv. Para proteger los intereses vitales del interesado

v. Para el cumplimiento de una misión realizada en el interés público

vi. Para satisfacer intereses legítimos del responsable o un tercero, siempre y cuando no interfiera con los intereses del titular.

Los anteriores supuestos, en caso de incumplimiento serán considerados como infracciones graves, de acuerdo con el artículo 72 del propio Reglamento.

b) Principio de lealtad.- El principio de lealtad consiste en que el responsable o el encargado del tratamiento, deberá ser leal con el titular de la información, para que no le dé un tratamiento diverso a la información, más allá para lo que fue solicitado.

c) Principio de transparencia.- Este principio salvaguarda el derecho de todo titular para conocer en todo momento la forma en que será tratada su información y podrá conocer de manera directa las intenciones del tratamiento, independientemente, si por razón de la propia empresa, se puede inferir de manera obvia. Lo anterior será accesible de primer momento a través del aviso de privacidad que se les proporcione a los titulares de la información, sin embargo, no queda limitado a prácticas que resulten más cómodas para informar al titular de la información.

d) Principio de minimización.- Los datos solicitados deberán de ser adecuados, pertinentes y limitados únicamente para cumplir con el fin para el que fueron solicitados y por lo que son tratados.

e) Principio de exactitud.- Este principio establece que es obligación de las empresas a que los datos deban ser exactos en todo momento y lo más actualizados posibles, por lo que se alienta a que se tomen medidas prácticas para que puedan actualizarse, o rectificarse en cualquier momento que sean necesarios.

f) Principio de limitación de plazo de conservación.- Este principio señala que los datos tratados por ningún motivo deberán de permanecer más tiempo del estipulado para cumplir con su finalidad, y estipula como

excepción únicamente los casos en que sean conservados para fines de archivo, de interés público, fines de investigación científica, histórica y/o estadística.

g) Principio de integridad y confidencialidad.- Este principio señala que deberán de mantenerse en todo momento los datos de una forma íntegra, la cual garantice que existirá una garantía de conservación, seguridad y confidencialidad para que no sea vulnerada o divulgada a terceras personas, cuando su titular no lo haya establecido concretamente, este principio se encuentra auxiliado por el artículo 39 que establece las medidas que deberán tomar las empresas para que no se vulnere la seguridad de la información; así como el artículo 49 que establece que deberá de contarse con adecuados estándares de seguridad que permitan cumplir con los objetivos del principio.
h) Responsabilidad proactiva.- Este principio señala que las empresas deberán de contar con una iniciativa y pro actividad que permita decidir sobre las mejores prácticas que tienen que implementar en sus organizaciones, y que estas les permitan garantizar una seguridad adecuada a los datos personales, incluyendo el tratamiento no autorizado o ilícito, su perdida, destrucción o daño accidental.

Muchos de los principios que ahora se señalan, tuvieron su origen desde la directiva 95/46/CE, la cual sirvió de base para afianzar sus objetivos y poder delimitar apropiadamente su alcance, también sirvieron de base numerosas normativas nacionales que tuvieron relación directa con la interpretación de estos principios y que pudieron aplicarlos a casos concretos, así como decisión del Tribunal de Justicia, la cual también contribuyó a establecer su alcance.

Con base en los principios señalados con antelación, es importante mencionar que ellos se formulan de modo breve en el artículo 5º del RGPD, sobre los principios aplicables a los tratamientos; sin embargo, es importante considerar que los principales responsables del cumplimiento de estos principios son las empresas y son los que deben ser capaces de demostrarlo, “esto significa, la

adopción de un nuevo enfoque, la responsabilidad proactiva, en la que la definición de los procesos de cumplimiento normativo, su documentación y mantenimiento resulta esencial[129]

Por otro lado, el RGPD, da facultades para que las empresas tomen el mando para dirigir de forma más flexible sus organizaciones y para que éstos realicen las adecuaciones necesarias para cumplir con dichos principios, por lo que también se ha llegado a afirmar que se "obliga a un enfoque basado en el riesgo. La pro actividad se encuentra al servicio de un derecho fundamental sometido a distintas presiones y susceptible de generar riesgos que afecten a la vida de las personas[130].

Por último, se considera relevante el cambiar de paradigma para proteger los derechos fundamentales, como han señalado varios autores expertos en privacidad "protegemos personas. Y esas personas nos confían su bien más valioso: su información personal, sus esperanzas de futuro[131]. Las empresas deberán de hacer su mayor esfuerzo para estar a la altura de cumplir con estos principios básicos y lograr transmitir esa confianza que el Reglamento persigue como uno de sus objetivos principales.

3.3.1. Derecho de acceso de información

El derecho de acceso a la información, nace dentro del RGPD con un objetivo, que la información pueda compartirse y que sea libre, así mismo, que para que la misma información pueda llegar a una serie de mercados que no conozcan fronteras entre países, ni fronteras entre economías[132].

Por lo anterior, de acuerdo con lo aseverado con algunos autores, "podemos destacar la obligatoriedad y la aplicación directa del Reglamento en los países de la Unión Europea, por lo que no necesita transposición y con ello,

[129] *Idem*.
[130] *Idem*.
[131] *Ibidem,* p.14
[132] De acuerdo con el considerando 12 del Reglamento de la Unión Europea (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 "El objetivo de la directiva es contribuir con el correcto funcionamiento del mercado interior, garantizando la libre circulación de los servicios de la sociedad de la información entre los Estados miembros".

acelera la eficacia de la aplicación de la norma en los Estados. Esta novedad trae como consecuencia la creación de un mercado único digital"[133]

España en su proyecto de Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales en su artículo 13 reconoce este derecho, haciendo especial énfasis en que ese derecho se ejercitará en todo momento en base a lo previsto por el RGPD en su artículo 15. Entre las adhesiones que se contemplan es la de solicitar información del afectado, cuándo éste, ejercitando su derecho de acceso de información, solicite gran cantidad de información sin especificar a qué datos se refiere. De igual forma, se agrega el apartado 4 a la Ley Orgánica, en la cual se autoriza el cobro de costes que deriven por la entrega de información, cuándo ésta rebase los medios y la forma en la que debe de ser entregada, el artículo 13.4 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales lo especifica de la siguiente manera: "Cuando el afectado elija un medio distinto al que se le ofrece que suponga un coste desproporcionado, la solicitud será considerada excesiva, por lo que dicho afectado asumirá el exceso de costes que su elección comporte. En este caso, solo será exigible al responsable del tratamiento la satisfacción del derecho de acceso sin dilaciones indebidas".

Sin perjuicio de lo anterior, la libre circulación de información y el acceso a la misma, que se ha cuidado en el Reglamento de la UE2016/679, también ha concebido dentro de su normativa una serie de excepciones, en los cuales no se aplicará de manera directa a los particulares en los siguientes casos:

- Cuando la información se utilice para actividades que no sean de aplicación directa a los miembros de la UE.
- Cuando la información sea utilizada por mandato judicial con el fin de investigar algún delito, o perseguir la seguridad de la población.

[133] Ortega Gimenez, Alfonso y Gonzalo Domenech, Juan José, "Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea", *Rev. Fac. Der. Online*, Montevideo, 2018, núm. 44, pp.31-73, *http://www.scielo.edu.uy/scielo.php?script=sci_arttext&pid=S2301066520180001000031&lng=es&nrm=iso>. ISSN 0797-8316. http://dx.doi.org/10.22187/rfd2018n44a2*

- Cuando se trate del "tratamiento de datos efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas[134]"[135]

Asimismo, también se protege a través del RGPD el principio de transparencia[136], el cual, a través del reglamento del RDPD se "refuerza la información que se debe facilitar a los titulares de los datos, tanto en el supuesto de que los datos se recaben directamente del interesado como si los datos se obtienen de otra fuente"[137]. En ese sentido la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales en su artículo 11 reconoce este derecho, pero lo deja a completo arbitrio del titular de la información de poder acceder a él o no, toda vez que en su inciso C, únicamente e agrega la posibilidad de ejercer el derecho si el titular así lo desea. Hago referencia a lo que el propio texto legislativo a la letra señala:

> Artículo 11. Transparencia e información al afectado.
> 1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información…
> **…c) "La posibilidad de ejercer** los derechos establecidos en los artículos 15 a 22 del Reglamento (UE) 2016/679.
> Si los datos obtenidos del afectado fueran a ser tratados para la elaboración de perfiles, la información básica comprenderá asimismo esta circunstancia. En este caso, el afectado deberá ser informado de su derecho a oponerse a la adopción de decisiones individuales automatizadas que **produzcan efectos jurídicos sobre él o le afecten significativamente de**

[134] De acuerdo con lo establecido en el propio Reglamento de la UE 2016/679, el mismo no tendrá aplicación cuándo se trate del tratamiento de datos de una persona física en el curso de una actividad exclusivamente personal o domestica, por tanto, sin conexión alguna con una actividad profesional o comerciante. Por motivo de lo anterior, se considera que solo tendrá aplicación para los responsables o encargados del tratamiento que proporcionen los medios para tratar los datos personales relacionados con tales actividades personales o domesticas.

[135] Ortega Giménez, Alfonso y Gonzalo Domenech, Juan José, *op. cit.*

[136] El principio de transparencia está considerado por el mismo reglamento con reglas básicas, como que toda información relativa al tratamiento de datos personales sea facilitado en todo momento a través de medios accesibles y mediante un lenguaje de fácil comprensión.

[137] Ortega Giménez, Alfonso y Gonzalo Domenech, Juan José, *op. cit.*

modo similar, cuando concurra este derecho de acuerdo con lo previsto en el artículo 22 del Reglamento (UE) 2016/679[138]

El acceso de información que regula el RGPD también ha considerado una serie de medidas que provocan que exista una responsabilidad directa para los sujetos que van a almacenar la información y permitirán el acceso y distribución de información, tal es el caso de las empresas; en esta ocasión, las empresas tendrán la obligación de notificar de manera pronta cualquier fallo de seguridad de los sistemas que resguardan la información, no sobrepasando de acuerdo con el artículo 33 del Reglamento de la UE 2016/679, de una plazo máximo de 72 horas[139]. El supuesto mencionado con antelación se encuentra regulado dentro del Reglamento, dentro del concepto de notificación de una violación de la seguridad de los datos personales a la autoridad de control. En el cual se trata de dar transparencia de todo tratamiento de información, es decir, dándole publicidad a cualquier acto que genere una fuga de datos de manera accidental o provocada, para que los titulares de esos datos, tengan en todo momento de que cómo están siendo tratados sus datos o si se encuentran en peligro. La notificación de toda fuga de información deberá de realizarse por parte del responsable o encargado del tratamiento de los datos a través del siguiente procedimiento[140]:

[138] Artículo 11 de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.

[139] De acuerdo con el artículo 33 del Reglamento de la Unión Europea (UE) 2016/679, se establece que: La notificación contemplada en el apartado 1 deberá, como mínimo: a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados; b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información; c) describir las posibles consecuencias de la violación de la seguridad de los datos personales; d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos. 4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

[140] Artículo 33 fracciones a, b, c, d, del Reglamento de la Unión Europea (UE) 2016/679

a) Describir de forma clara el tipo de violación de seguridad de los datos personales[141].
b) Proporcionar los datos del delegado de protección de datos personales asignado para que pueda estar en comunicación constante con los interesados o afectados directos de la fuga de datos.
c) Describir de manera general un estimado de las posibles consecuencias por motivo de las violaciones a la seguridad de la información.
d) Señalar las medidas adaptadas hasta ese momento y el plan de acción propuesto para mitigar efectos negativos.

Con lo anterior, "se hace más estricta la necesidad de consentimiento de los afectados para el tratamiento de sus datos, limitando el consentimiento tácito y creando nuevas categorías de datos sensibles como los datos biométricos que requerirán un consentimiento reforzado"[142]. A pesar de la importancia de este artículo se puede notar que la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales de España no implementa este supuesto en su texto legal, toda vez que no está prevista como tal en su legislación vigente.

3.3.2. Derecho de portabilidad

El derecho de portabilidad ha nacido directamente con los avances tecnológicos que se han experimentado los inevitables desarrollos de hardware y software, así como de los servicios que se proporcionan a través de la llamada nube, han hecho que éstos a través de la red colaborativa que es el Internet, crearán unas nuevas formas de interacción y comunicación humana, creando los sitios webs, las denominadas redes sociales y la interacción múltiple en la que se permite que se cualquier usuario participe, difunda y comparta información.

---

[141] De acuerdo con el artículo 34 del Reglamento de la Unión Europea (UE) 2016/679, la comunicación deberá de darse en un lenguaje claro y sencillo y no será aplicable en los siguientes casos: a) Si el responsable ya ha adoptado medidas que hagan inteligibles los datos, por ejemplo, el cifrado, b) El responsable de los datos haya tomado medidas que le permitieran mitigar los daños causados y que garanticen que ya no se corre riesgo, c) La comunicación sea imposible o desproporcionada, por lo que se adoptarán medidas alternas como las comunicaciones públicas.

[142] Ortega Giménez, Alfonso y Gonzalo Domenech, Juan José, *op. cit.*

Lo anterior ha provocado el estudio de cómo es la forma en que se comparte la información y sus principales consecuencias, Puccinelli señala al respecto:

> Esta nueva realidad trajo consigo una marcada preocupación por el manejo de los datos personales implicados en dichas operaciones, en especial por cuanto los derechos expresamente reconocidos a los titulares de los datos en las normas nacionales y comunitarias sobre protección de datos vigentes por entonces aparecían insuficientes para enfrentar una Internet en constante despliegue[143]

Se considera a la portabilidad de la información como "un elemento esencial de la nueva economía digital y también del gobierno abierto, ya que los desarrollos privados y públicos reposan cada vez en mayor medida en la disposición de datos en formatos que permitan la interoperabilidad de los sistemas de información, pieza clave de la sociedad del conocimiento"[144]. Es decir, al día de hoy, la forma en la cual puede disponerse de grandes bases de datos, es imprescindible para medir el valor de una empresa, por lo que deberá de cuidar la forma en cómo maneja la información que tiene en su poder.

Este derecho ha demostrado dar una serie de prerrogativas que de manera directa benefician a los titulares de la información, así como a las empresas que se han dedicado a crear a partir de la recolección de información su principal fuente de activos, toda vez que se ha afirmado que "Intuitivamente el derecho a la portabilidad de los datos parece aportar mecanismos efectivos de protección frente al desarrollo de servicios y modelos de negocio que se han generado en torno a la red"[145]

De acuerdo con el propio RGPD, el derecho a la portabilidad está contemplado de manera directa dentro del mismo, ubicándose en su artículo 20, que enuncia la forma en que deberá el titular de la información hacerlo valer.

Se señala en todo momento que el titular de la información podrá requerir al sujeto o institución que resguarde su información, en cualquier momento que

---

[143] Puccinelli Oscar, Raúl, "El derecho a la portabilidad de los datos personales. Orígenes, sentido y alcances" *Revista Pensamiento Constitucional*, vol. 22, núm. 22, p.208,http://revistas.pucp.edu.pe/index.php/pensamientoconstitucional/article/view/19945/19966

[144] *Idem.*

[145] Miralles, Ramón, *El derecho de la portabilidad de los datos personales*, 2012, http://www.abogacia.es/2012/11/15/el-derecho-de-la-portabilidad-de-los-datos-personales

desee, los datos que fueron proporcionados en su momento, “proporcionados por el titular al responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado”[146]

Por otro lado, también el RGPD, considera la opción de que el consentimiento del tratamiento de información se haya dado desde un inicio por medio de datos automatizados. Para tal situación el reglamento contempla que se intentará en todo momento recuperar y transmitir los datos de responsable a responsable hasta que puedan proporcionarse a destinatario que señale el titular de la información.

Como excepciones a este derecho de portabilidad, la transmisión de la información no se podrá realizar por ningún motivo cuando éstos se hagan para satisfacer un interés público; por lo que, sólo será permitido recibir datos personales y que el nuevo responsable los almacene y resguarde para su uso personal, siempre cuando no se transmita a otro responsable.

Los datos personales que se consideran dentro de este supuesto, y que están sujetos a la portabilidad son los que directamente se proporcionan por el titular de la información, tal es el caso de la dirección postal, nombre de usuario y edad, así como de los datos que son “proporcionados por el interesado en virtud del uso del servicio o del dispositivo (historial de búsqueda, datos de tráfico o datos de localización). Sin embargo, los datos inferidos y derivados, por cuanto que son creados por el responsable sobre la base de los datos proporcionados por el interesado, no entrarán dentro del ámbito del derecho a la portabilidad de datos”[147].

Es importante comenzar a considerar las ventajas y desventajas que traerá consigo este nuevo derecho, así como los retos que se imponen a las empresas que manejan gran cantidad de información, por lo que deberán de pensar en una

---

[146] *Idem*.

[147] Ortega Gimenez, Alfonso y Gonzalo Domenech, Juan José, “Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea”, *Rev. Fac. Der.* Online, Montevideo, núm.44 2018, pp.31-73. *http://www.scielo.edu.uy/scielo.php?script=sci_arttext&pid=S2301066520180001000031&lng=es&nrm=iso>. ISSN 0797-8316. http://dx.doi.org/10.22187/rfd2018n44a2*

manera clara y accesible para poder llevar a cabo esta labor. Por mencionar algunos ejemplos, Puccinelli señala al respecto:

> resulta difícil imaginar hasta qué punto el cliente de un servicio de banca en línea podrá ejercer su derecho a transmitir su información a otra entidad financiera, o por ejemplo, lo interesante que sería que un vendedor de productos en línea pudiera transferir la información de su perfil de ventas (en definitiva su prestigio digital como vendedor) a otra plataforma de subastas, y no tener que empezar desde cero a generar confianza en los compradores de la nueva plataforma a la que se ha trasladado[148]

Considerando a éste, uno de los nuevos retos de interpretación y cumplimiento que traerá el derecho de portabilidad en la protección de datos, no debe dejarse de lado el avance regulatorio que dentro de las tecnologías de la información se han creado, toda vez que "tanto por su incidencia práctica como por su complejidad técnica, que están incorporando las legislaciones más recientes"[149] se comiencen a regular nuevos derechos derivados directamente de las TICs.

3.3.3. Libertad de información

La libertad de información, se refiere a la forma en que una persona podrá disponer de su propia información de carácter personal, y de la forma en la que autorizará o negará que sea utilizada la misma, para los fines que el conozca y permita previamente.

Este derecho toma su relevancia dentro del comercio electrónico, toda vez que se consideró el problema social que derivó del masivo acceso y distribución de la información con la que disponían los prestadores de servicios principalmente. En tales situaciones, los prestadores de servicio, disponían de esa información para realizar prácticas comerciales muchas veces no autorizadas por los titulares de la información, tal es el caso de la actividad publicitaria.

---

[148] Puccinelli Oscar, Raúl, "El derecho a la portabilidad de los datos personales. Orígenes, sentido y alcances" *Revista Pensamiento Constitucion*al, vol. 22, núm. 22, p.211,*http://revistas.pucp.edu.pe/index.php/pensamientoconstitucional/article/view/19945/19966*

[149] *Ibidem*, p.228.

De acuerdo con lo señalado por la autora Presas Mata “la actividad publicitaria, como parte del proceso de comunicación, no se desarrolla solo con el objetivo de informar, sino que busca diferenciarse a través de los valores de marca. Estimula, incita, provoca con el fin de generar una reacción en el receptor del mensaje e inducir la compra”[150]. Es decir, los mismos prestadores de servicios, sacan provecho de toda la información de carácter personal con la que disponen para poder hacer crecer sus negocios de manera indirecta, y utilizan los medios electrónicos porque son medios accesibles de distribución de información.

“La publicidad actual se sitúa en el contexto de la sociedad de la información y del conocimiento, en el que es impensable diferenciar al producto por sus cualidades físicas y por ello busca la distinción en sus atributos simbólicos.”[151]. Es por lo anterior que la directiva busca regular y parar un poco con la práctica desmedida que se realiza sin el consentimiento directo de los titulares de la información.

La libertad de la información, permitirá que los titulares de los datos personales, decidan de manera directa y consciente la forma en la que permitirán que su información transcienda y que sea utilizada, así como decidir en qué actividades se encuentra su información.

3.3.4. Control de información

El control de información como derecho dentro del Reglamento General de Datos Personales, permitirá tener un control directo con respecto al posicionamiento de las prácticas publicitarias, toda vez que el uso no autorizado de información provoca que “los contenidos publicitarios se presenten con relativa frecuencia por medio de mensajes que impiden advertir claramente la veracidad o falsedad de los argumentos y propuestas”[152]

---

[150] Presas Mata, Fátima, “La responsabilidad social de los skateholders en la publicidad: necesidad de un compromiso ético en la industria publicitaria”, M*ethaodos, Revista de ciencias sociales*, Vigo, vol. 6, núm. 1, 2018, p. 40.

[151] *Idem.*

[152] *Ibidem*, p. 45

Un adecuado control de información permitirá que la publicidad se desarrolle de manera adecuada y profesional conforme a normas éticas que se dispongan a través de la ley, y que éstas no impidan de manera directa el ejercicio de la libertad de información, sino todo lo contrario. “Anunciantes, agencias y medios deben actuar con total libertad, pero es preciso delimitar que la libertad no es la ausencia de reglas”[153]

Para que la protección de información se pueda llevar a cabo desde el principio de control de información, es necesaria que exista una figura que dé cabal cumplimiento a ese control de información, la cual deberá de ser una persona encargada directamente a velar y proteger el debido cumplimento tanto de la información de carácter personal que se trate, como de las disposiciones que el RGPD señale.

La Responsabilidad que tomarán los nuevos responsables del control de la información, debe de distinguirse en tareas con las actividades que habían estado tomando un responsable en seguridad de información, toda vez que son actividades completamente diferentes y que ameritarán un compromiso diferente en objetivos y tareas diarias

La diferencia más notoria entre el Responsable de Seguridad y el DPO es la exclusividad de éste último en sus funciones, el DPO ya no será como hasta ahora la persona que se designaba como Responsable de Seguridad, ocurriendo que, sin apenas justificación, “se elegía al informático o se auto nombraba el administrativo al que su jefe le derivó informarse sobre cómo cumplir con la LOPD en la empresa, es por ello que esta nueva figura supone reforzar la cultura del *compliance* en materia de protección de datos”[154]

---

[153] *Ibidem*, p. 46

[154] Ortega Gimenez, Alfonso y Gonzalo Domenech, Juan José, “Nuevo marco jurídico en materia de protección de datos de carácter personal en la Unión Europea”, *Rev. Fac. Der.* Online, Montevideo, 2018, núm. 44, pp. 31-73, *http://www.scielo.edu.uy/scielo.php?script=sci_arttext&pid=S2301066520180001000031&lng=es&nrm=iso>. ISSN 0797-8316. http://dx.doi.org/10.22187/rfd2018n44a2*

3.3.5. Derecho de supresión de datos (Derecho al olvido)

El derecho al olvido ha tenido en los últimos años una importante aparición a raíz de la iniciativa social de proteger la información. Este derecho tuvo sus orígenes en Europa, sin embargo, tiene alcance internacional, toda vez que las legislaciones de otros países del mundo han optado por contemplarlo en sus legislaciones.

Se le conoce como el derecho al olvido, término conocido generalmente, o derecho al borrado como resulta más adecuado en la práctica por algunos autores. Por su parte, la AEPD lo ha definido "como el derecho a impedir la difusión de información personal a través de Internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa"[155]. En otras palabras, este derecho permite limitar la difusión universal e indiscriminada de datos personales en los principales motores de búsqueda cuando la información, por razón del trascurso del tiempo se convierte en obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima.

Originalmente este derecho no estaba reconocido en la Directiva 95/46/CE de la UE, pero no por eso se considera para poder regularlo, por lo que la Sentencia de la Gran Sala del Tribunal de Justicia de la UE de 2014 sobre el asunto C-131/12 dio vista a este derecho, aún y cuando no existía como derecho, lo que provocó que no se interpretara de manera correcta.

En virtud de tal situación, la Ley General de Protección de Información, al incorporar el derecho al olvido en su normatividad, estableció estándares mínimos y ejemplos en los cuales deberá de respetarse y hacerse cumplir la normatividad.

1. Por un lado, se estableció que la actividad de un motor de búsqueda, el cual consiste en encontrar de manera automatizada información publicada o puesta en Internet por terceros, almacenarla, y ponerla a disposición de los internautas, según un orden de preferencia determinado, debe considerarse un tratamiento de datos personales, por

[155] *Idem*

lo que, ese mismo responsable del motor de búsqueda debe ser responsable directo del tratamiento de esos datos.

2. Por otro lado, se estableció que cuando el gestor de un motor de búsqueda crea en algún Estado miembro una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro, que entiende que se lleva a cabo un tratamiento de datos personales en el marco de las actividades de un establecimiento del responsable de dicho tratamiento en territorio de un Estado miembro.
3. Se establece que de manera general el gestor de un motor de búsqueda estará obligado en todo momento a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a la persona en cuestión, así como en el caso de que ese nombre o la información no se borren de manera previa o simultáneamente de las páginas web, aunque se disponga que las mismas páginas contiene información lícita.
4. Deberá examinarse en todo momento y de manera especial si el titular dispone de manera fehaciente a que su información ya no esté en la situación actual, la vinculación a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre, sin que la apreciación de la existencia de tal derecho presuponga que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado.

De manera concreta, el RGPD, reconoce en todo momento el derecho al olvido de la siguiente forma:

1. El interesado tendrá derecho a obtener sin contratiempos ni excusas indebidas por parte del responsable del tratamiento de su información de

carácter personal, a la supresión de sus datos personales y éste último deberá de suprimir sin dilación.

2. Cuando por el mal uso de datos personales el encargado de la información incurra en alguna circunstancia no autorizada como es el fin del uso de los datos, retire el consentimiento, se oponga a su tratamiento, sea una obligación exigible por la Unión o por los Estados o los datos se hayan obtenido por una oferta de servicios de la sociedad de la información.
3. Los responsables de la información deberán de tener con toda la tecnología y medios necesarios para el correcto cumplimiento de las solicitudes correspondientes en caso de que les sean requeridas.

Como excepción a lo anterior, el RGPD contempla que no existirá derecho al olvido cuando se haga en pro de la libertad de información, o cuando se dé cumplimiento a una obligación legal, así como que la información sea necesaria para el interés público, información histórica o estadística, y para acciones de defensa.

> Habrá entonces un nuevo «derecho al olvido digital» («RTBF 2.0»), que se corresponde con la versión receptada por el Superior Tribunal de Justicia de la Unión Europea en el célebre caso «Costeja»12, concebido como un modo de inhibir el acceso, a través de los buscadores de Internet, a datos ciertos que originalmente fueron lícitamente publicados pero que por el paso del tiempo perdieron toda relevancia pública, en una suerte de «borrado» de los rastros de un pasado que se desea olvidar del cual su protagonista se encuentra prisionero, por efecto de una Internet que, a diferencia del ser humano, no olvida y en la cual el tiempo, a diferencia del tiempo humano, se detiene[156]

Derivado de lo anterior, es importante reconocer no solo las obligaciones que incorpora la legislación internacional, sino también conocer los nuevos derechos que son reconocidos, así como las excepciones que ahora se contemplan, siempre en pro de la libertad de expresión y acceso de información.

[156] *Ibidem*, p. 209

3.4. La regulación internacional del Reglamento General de Protección de Datos dentro de la Unión Europea, estudio comparativo

Uno de los principales objetivos del Reglamento de la UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, adicional al más importante que es el de la protección de datos de carácter personal, es la homogenización y creación de un derecho uniforme que permita la armonización entre los países miembros que componen la UE, esto, para trabajar de manera conjunta en el principal objetivo del Reglamento.

Por motivo de lo anterior, los países miembros de la UE, además de España, han trabajado en el ajuste de sus legislaciones internas para adecuar las normativas que hasta ese momento tenían vigentes en materia de protección de datos personales. Algunos de los países de la UE que ya cuentan con legislación propia en la materia son Alemania, Bélgica, Gran Bretaña, Francia e Italia. Algunos de ellos han apoyado a elaborar y aportar información y normas relevantes al Reglamento y otras han modificados en base al Reglamento a su propia normativa nacional[157].

Alemania. Considerado en todo momento como país pionero en materia de protección de datos ha realizado la aprobación el 30 junio del año 2017 de la Ley *Act to Adapt Data protectionLaw to regulation (EU) 2016/679 and to ImplementDirective (EU) 2016/680*, en la que se han adaptado las principales disposiciones en la materia en Alemania, basados en la propia directiva de UE.

Bélgica. Este país por su parte ha contribuido con el Reglamento a través de su normativa denominada *Loirelative à la protection de la vie privée à l'égard des traitements de données à caractèrepersonnel,* de 8 de diciembre de 1992, el cual ha servido de bases para varios principios que están plasmados en el Reglamento de la UE.

Francia. Para este país el Reglamento de la UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 ha contribuido significativamente en la aportación del texto normativo para poder actualizar y ajustar su propia normativa interna en materia de privacidad y protección de datos personales, por

[157]*DOSIERES*, Congreso de diputados, diciembre 2017, XII Legislatura, núm. 13.

lo que, se ha derivado la modificación de varias textos legislativos del país, tal es el caso de La *Loi 78-17 du 6 janvier relative à l'informatique, auxfichiers et auxlibertés*, haciendo especial énfasis en los artículos 1, 32, 40-1 o 43; y de algunas disposiciones introducidas en la *Loi nº 2016-1321 du 7 octobre 2016 pour une République numérique*. Asimismo, Francia realizó un informe de la Asamblea Nacional[158], donde detalla todas las adhesiones que realiza en su legislación en materia de protección de datos personales.

Italia. Este país ha contribuido a la creación del Reglamento de la UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, con las implementaciones de las aportaciones contenidas en su *Codice in materia dim protezione dei dati personali*[159]. Asimismo, una vez aprobado el Reglamento de la UE, Italia realizó el texto denominado *Guida all applicazione del Reglamento UE 2016/679,* en el cual, se hace un análisis de todos los cambios que traerá consigo la nueva normativa de datos de la UE a la propia legislación Italiana.

Gran Bretaña. Este país ha realizado la valoración de lo contenido en el Reglamento de la UE 2016/679, y está en creación del documento denominado *Data Protection Bill,* en el cual, valoran los principales cambios que son urgentes realizar en su legislación para cumplir con el Reglamento y con el documento denominado *Explanatory Notes*, pretenden explicar los principales cambios para que sean de fácil compresión. También han trabajado en la elaboración del documento denominado *Briefing de la Cámara de los Lores,* el cual será una evaluación para la aprobación del proyecto.

Portugal. Este país no dispone de una legislación concreta en materia de protección de datos, por lo que, se ha tomado hasta este momento en sentido de análisis y de referencia a los textos contenidos en la *Comissão Nacional de Protecção de Dados[160] (CNPD).* Esta comisión es la encargada a nivel nacional de regular todo lo concerniente a la protección de datos y este último año ha

[158] Comisión de Derecho Constitucional*, Las implicaciones de las nuevas normas europeas para la Protección de datos personales en derecho Francés*. Informe de 4544 de la Comisión de Derecho Constitucional, Legislación y Administración General de la República. Asamblea Nacional, 22 de febrero de 2017.

[159] Texto aprobado mediante Decreto legislativo en 2003.

[160] Comisión Nacional de Protección de Datos.

aprobado el Reglamento número 1/2018 en el que se hace una evaluación del impacto del del Reglamento de la UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, considerando los cambios que son indispensables realizar para su correcto cumplimiento frente la UE.

Es importante destacar que aunque se considere al Reglamento de la UE 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, como el máximo regulador de datos dentro de la UE, se considera indispensable que cada uno de los Estados Miembros tomen como base lo contenido en el reglamento, pero que a su vez, diseñen de acuerdo a las necesidades de su población, elementos tecnológicos y legales y su propio ambiente comercial, las medidas necesarias para aplicar correctamente lo establecido por el propio reglamento, es decir, que adecuen lo establecido en el Reglamento a sus propias necesidades, respetando en todo momento las finalidades primordiales de protección que exige el texto legal.

3.5. Ejercicio comparativo de normativas legales en materia de protección de datos para el e-commerce: RGPD y LFPDPPP

El RGPD ha llevado a cabo la implementación de un nuevo paradigma en cuestión de protección de datos personales; la misma UE ha reconocido que se encuentra en un momento crucial de evolución y con retos enormes a cumplir, a pesar de haber contado con un *vacatio legis* de dos años, se ha señalado que "sobre ese reto que el RGPD ha venido a planteara los Estados miembros, el de garantizar un ajuste armónico entre el acervo nacional en la materia y el RGPD"[161], lo más difícil será la implementación a la normativa nacional, sin embargo también reconocen que no es la primera vez que eso sucede, toda vez que es normal que el derecho comunitario goce de efectos directos por sobre encima de los propios derechos nacionales de los países miembros de la UE.

[161] García Mexía, Pablo, "*La singular naturaleza jurídica del reglamento general de protección de datos de la UE, sus efectos en el acervo nacional sobre protección de Datos", en* Piñar Mañas, José (Dir.), *Reglamento general de protección de datos*, Reus, Madrid, 2017, p. 30.

Desde el punto de vista de los propios países que componen la UE, éstos se han encontrado con diversos retos para adaptar el reglamento a sus legislaciones internas, un ejemplo claro en España fue la reforma completa de su anterior LOPD para suplirla con la nueva normativa que se encuentra en aplicación y suprimiendo cosas antes consideradas tan importantes como la obligación en España de notificar la creación de ficheros e inscripción ante el Registro general de protección de Datos, ahora se apuesta más por la autorregulación de los entes responsables de la información, ya que deberán de seguir organizándola y resguardándola correctamente, sin embargo, solo tendrán la obligación de mostrarla o presentarla cuando la autoridad de control así se lo solicite, de acuerdo con lo señalado por el artículo 30.4 del RGPD.

Desde el momento en que se llevó a cabo la presentación del RGPD, autores como García Mexía reconocieron la importancia que era adaptar su ordenamiento de acuerdo con lo que señalaba el propio reglamento, aseverando lo siguiente:

> El legislador que en España deba acometer la adaptación de nuestro acervo nacional sobre protección de datos al RGPD (pues quiero creer que efectivamente se optará por hacerlo), no deberá cometer esos mismos errores. Deberá facilitar la adaptación, no oscurecerla; deberá propiciar la aplicación directa del RGPD (que es lo que en el fondo la UE ha dispuesto), no entorpecerla[162].

Lo anterior, entre otras cuestiones, hizo que uno de los países que componen el núcleo activo de la UE, realizaran importantes modificaciones internas para estar en posibilidad de cumplir con los ordenamientos que estipula la propia UE; sin embargo, se realiza el siguiente cuestionamiento: ¿qué pasa con el ámbito territorial de aplicación para los países terceros que no son propiamente parte de la Comunidad Europea?

La UE se ha encontrado desde la aplicación de la Directiva 95/46/CE con varios conflictos de interpretación con respecto a la aplicación territorial de la norma, el asunto C-131/12 (*Google Spain*) hizo que la comunidad Europea

[162] *Ibidem*, p. 34.

repensará y reforzará sus lineamientos de aplicación y dio como consecuencia que el RGPD entre otras cosas estipulara dentro de su artículo 3º lo siguiente:

> 1. El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado del tratamiento en la Unión.
> 2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable del tratamiento no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:
> a) la oferta de bienes o servicios a dichos interesados en la Unión; o
> b) el control de su conducta.
> 3. El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable del tratamiento que no esté establecido en la Unión sino en un lugar en que sea de aplicación la legislación nacional de un Estado miembro en virtud del Derecho internacional público.[163]

Lo anterior señala de manera puntual dos fundamentos que cualquier empresa o ente gubernamental que quiera realizar relaciones con las comunidad Europea tiene que considerar. El primero de ellos es que no importa si se trata de un país tercero ajeno a la UE, siempre que éste tenga el estatus de encargado o de responsable de los datos que recabe; y la segunda cuestión que encuadra directamente, es el hecho de que las actividades que derivan del comercio electrónico son principalmente la oferta de bienes y servicios y cuando estos tienen como finalidad vender a alguno de los ciudadanos miembros de la UE.

El propio RGPD en su considerando número 23 establece que:

> Para determinar si dicho responsable o encargado ofrece bienes o servicios a interesados que residan en la Unión, debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios Estados miembros. Son factores que permiten determinar esta intención que el sitio web del responsable o encargado, o de su intermediario en la UE, use una lengua o una moneda generalmente utilizada en uno o varios Estados miembros, con la posibilidad de ofrecer bienes o servicios en esa lengua, además de la lengua generalmente utilizada en el tercer país donde resida. O bien que el sitio web haga mención de clientes o usuarios que residen en la UE

[163] Ripol Carulla, Santiago, "Aplicación territorial del Reglamento" *en* Piñar Mañas, José (Dir.), *Reglamento general de protección de datos*, Reus, Madrid, 2017, pp. 93-95.

Tomando en consideración las anteriores referencias, México queda completamente encuadrado si se considera que podría ofrecer a través del comercio electrónico productos y servicios a España, quien coincide en lengua y que con la ayuda de las tecnologías de la información y comunicaciones, a través del Internet puede llegar a lugares y personas que pertenezcan a esa comunidad. Y en virtud de lo anterior es importante preguntarnos en ¿qué posición se encuentra México para poder considerar que efectivamente está en posibilidades de cumplir con el RGPD?, claro está, partiendo de la premisa de que ejercerá el comercio electrónico a alguno de los países miembros de la UE, o que como consecuencia de su actividad comercial, tratará datos de algún miembro que sea parte de la propia UE.

Ahora bien, considerando la anterior aseveración, las empresas mexicanas dedicadas al *e-commerce* trasnacional, principalmente al europeo deberán de considerar no solo lo referente a la LFPDPPP sino también a lo que señala el RGPD, de primera instancia se puede dilucidad dentro del propio texto de la LFPDPPP que tiene varias disposiciones similares a las que señala el RPGD, tal es el caso de:

1. El reconocimiento de los derechos de acceso, rectificación, cancelación y oposición de los datos personales (Derechos ARCO):
2. Los mecanismos para asegurar los derechos ARCO.
3. Evaluación y análisis del flujo de datos personales y su tratamiento.
4. Las figuras de responsables y encargados del tratamiento, así como sus principales obligaciones.
5. La obligación de la elaboración de avisos de privacidad y el contenido mínimo que deberá de estipularse en cada uno de ellos.

Por otro lado, existen disposiciones que repercuten directamente con las diferencias que existen en la LFPDPPP con respecto al RGPD, y que no contempla en su texto legal, alguno de estos casos son los siguientes:

1. Las medidas de seguridad en el RGPD, son más detalladas y precisas en cuestión del procedimiento a emplear, algo con lo que no cuenta la LFPDPPP.
2. El tiempo en que están obligados los responsables y/o encargados de los datos personales de notificar a los titulares de la información y a las autoridades competentes en caso de que sean víctimas de vulneraciones o incidencias de seguridad.
3. En el caso del consentimiento para el tratamiento de información, la LFPDPPP contempla el consentimiento tácito, sin embargo el RGPD, ha cambiado considerablemente esta disposición, señalando que únicamente podrán tratarse los datos personales cuando el titular expresamente lo apruebe.
4. El derecho de supresión de datos (derecho al olvido) no está contemplado en la LFPDPPP.
5. La protección de datos utilizando las estrategias tecnológicas de diseño y por defecto, tampoco es un tema que expresamente recomiende la LFPDPPP para proteger los datos personales, recomendaciones que hacen de manera expresa en el RGPD.

En virtud de lo anterior y aunque la legislación mexicana a través del LFPDPPP cuente con obligaciones similares detalladas en el RGPD, no es suficiente con el cumplimiento de esta ley, si el objetivo es expandirse al mercado europeo, sobre todo cuando se trate de datos personales de algún miembro de la UE.

Cualquier empresa que trate información de algún miembro de la UE o que tenga como principal objetivo ofrecer productos o servicios a la propia UE, deberá primeramente de cumplir con lo que la legislación nacional aplicable señale al respecto, pero también deberá de conocer las disposiciones que emanan del RGPD para adaptar las medidas de protección que el reglamento exige. Aunque la normativa se encuentra en constante adaptación y cambios de disposiciones internacionales, los *e-commerce* mexicanos que deseen ofrecer productos y/o

servicios al mercado europeo, no pueden esperarse a que se regularice dentro de la normativa internacional todas estas disposiciones, toda vez que no se ha conocido una fecha específica en el que esto ocurrirá.

Tal y como señala Colmenarejo Fernández en líneas que me permito transcribir a continuación:

> Los ciudadanos ya no pactamos las condiciones de nuestra seguridad con el estado, como dejó planteado Hobbes en su Leviatán (1651), sino con nuestro proveedor de datos, quien nos da acceso a la sociedad red. La cuestión estriba ahora en estimar el alcance de nuestro accesoa las cláusulas de dicho contrato y en dilucidar si nuestra posición como sujetos morales es bien como profesionales, ciudadanos/as o como clientes y/o proveedores[164]

Aterrizando la interpretación a nuestro tema de estudio, lo que la autora desea dar a entender es que la cooperación de diferentes entes inmiscuidos en la protección de información, así como de sujetos obligados, es la mejor opción para brindar un compromiso de cumplimiento acertado y sobretodo eficaz, la autorregulación es imprescindible para que se cumpla de una manera adecuada con la ley y, los principales interesados en tal disposición serán las empresas como tal, pues el incumplimiento no será aplicable al estado, sino a las mismas empresas, he ahí la importancia de la observancia de ambas normativas.

[164] Colmenarejo Fernández, Rosa, *Una ética para Big data: introducción a la gestión ética de datos masivos*, Barcelona, UOC, 2018, p. 18.

CAPÍTULO 4
LA PROTECCIÓN DE DATOS PERSONALES A TRAVÉS DE PRESTADORES DE SERVICIOS ENFOCADOS AL E-COMMERCE: CASO MÉXICO

SUMARIO: *4.1. El comercio electrónico en México; 4.2. El comercio internacional electrónico en México. 4.3. El tratamiento de datos personales por empresas transnacionales que operan en México; 4.4. El tratamiento de datos personales por micros, pequeñas y medianas empresas; 4.5. Los problemas de aplicación de la normativa interna para protección de datos personales a los actos realizados a través del e-commerce en México; 4.6. Alternativas para un adecuado cumplimiento a la protección de información de carácter personal del e-commerce en México a través de las tecnologías de la Información*

El comercio electrónico en México es una actividad económica en vías de crecimiento, su reconocimiento e implementación tanto por empresas nacionales como extranjeras, ha hecho que evolucione la forma en que se crean relaciones comerciales en el país dentro y fuera de sus fronteras. En el presente capítulo se identificará la posición del comercio electrónico en México, así como las medidas legales y tecnológicas que las empresas dedicadas al sector deben de comenzar a implementar para cumplir satisfactoriamente con los requisitos que solicita la UE para crear lazos comerciales entre naciones.

4.1. El comercio electrónico en México

El contenido del comercio en México varía de acuerdo a las costumbres y la literalidad de cada uno de los autores que se han dedicado al estudio del tema. Como pudo apreciarse durante esta investigación es difícil tener una definición universal para su interpretación, ya que engloba un conjunto de características,

objetivos y elementos que cada persona, organización y país interpreta y aplica en su vida diaria; por su parte en México se ha llegado a aseverar a través de autores como Gaytán Torres como "la rama de la actividad económica que se refiere al intercambio de mercancías y servicios, mediante trueque o dinero, con fines de reventa o para satisfacer necesidades"[165].

Partiendo de la propia definición de lo considerado en México como comercio, el CCo -en su artículo 3°, fracción primera- establece que se consideraran como comerciantes "las personas que, teniendo capacidad legal para ejercer el comercio, hacen de él su ocupación ordinaria".

Sin embargo, esto no debe de considerarse únicamente como actividades que realiza un determinado grupo de personas que se envistan de tal calidad, como en el caso de las empresas ya que "no sólo el empresario debe dedicarse a actividades que se consideren mercantiles, esto es, que puedan englobarse dentro del concepto de comercio*"[166].*

Esto ha quedado más que señalado por nuestra legislación mexicana, quien en su artículo 4° del CCo establece que "las personas que accidentalmente, con o sin establecimiento fijo, hagan alguna operación de comercio, aunque no son en derecho comerciantes, quedan sin embargo sujetas a las leyes mercantile*s".*

Lo anterior, nos da una pauta para comprender que ningún ciudadano está eximido de ser sujeto de las leyes mercantiles mexicanas con respecto al cumplimiento de las disposiciones del comercio, ya que diariamente se realizan operaciones, transacciones o actos que indirectamente lo incluyen en el ámbito del comercio.

Con la revolución tecnológica que se experimenta actualmente a través de la sociedad de la información, se produjo a la necesidad de evolucionar en ciertas actividades cotidianas, la forma en que se realizan actividades de comercio no fue la excepción, por lo que, con la utilización del Internet, surgió lo que conoce como comercio electrónico.

Por otro lado, al acercarnos a conocer una definición legal de la palabra

[165] Gaytán Torres, Ricardo, *Teoría del comercio internacional*, 25ª ed., México, Siglo XXI, 2005, p.11.
[166] López Sánchez, Manuel Ángel, *Derecho mercantil I*, Pamplona, 2009, p. 85.

comercio electrónico, se aprecia que el CCo, hace una cantidad considerable de definiciones que están relacionadas con la palabra comercio electrónico, sin embargo, de los anteriores ejemplos, la palabra comercio electrónico nunca tiene una definición como tal, por lo que, se ha considerado apropiado investigar la definición de la palabra desde el punto de vista de un mensaje de datos.

De acuerdo con el artículo 89 del CCo, los mensajes de datos son toda "información generada, enviada, recibida o archivada por medios electrónicos, ópticos de cualquier otra tecnología" .En tal situación, aunque es claro que estos no solo se refieren a los proporcionados por el Internet, ni únicamente para el comercio electrónico, en México, es lo más cercano que el CCo ofrece al tema.

Por otro lado, tomando como referencia lo señalado por Pendón Meléndez con respecto al comercio electrónico, de que es una forma más en la que se lleva a cabo una transacción mercantil, más no una forma completamente aislada e independiente del tema; puede afirmarse que hoy en día se regulan gran parte de los actos realizados a través del comercio electrónico apoyándose en lo que las legislaciones actuales en México ofrecen al respecto, tal es el caso de la Ley Federal del Consumidor, la IFT, Ley Federal de Derechos de Autor, Ley Federal de la Propiedad Industrial, el CCo y la LFPDPPP por mencionar algunos ejemplos.

En supuesto de que se presente alguna queja por parte de un ciberconsumidor a un prestador de servicios a través de comercio electrónico, la Ley Federal del Consumidor a través de la Procuraduría Federal del Consumidor (PROFECO), tiene facultades para conocer y dar vista al asunto; si se solicita la regulación del contenido de una página de Internet que ofrezca directamente actividades de comercio electrónico deberá apoyarse en lo que señala la Ley Federal de Derechos de Autor al respecto, a través del INDAUTOR; lo concerniente a marcas y registros que estén contenidos en una página de Internet regulada en el comercio electrónico podrá solicitarse su protección a través de la Ley de Propiedad Industrial a través del IMPI, los actos de comercio entre empresas y/o personas físicas que tomen la calidad de comerciantes, podrán apoyarse de acuerdo a lo que señala el CCo; inclusive si es necesario dirimir alguna controversia derivada de la emisión de comprobantes fiscales, la

efectividad y validez de la firma electrónica o el uso de la firma electrónico avanzada dentro del comercio electrónico, podrá resolverse a través de lo que el Código Fiscal de la Federación pronuncia al respecto.

Es menester mencionar la importancia que tiene la LFPDPPP, el cual, como legislación de carácter nacional vela por la protección de los datos personales en posesión de los particulares, cuando se estos se tratan a través de actividades mercantiles, y precisamente, a través de actividades mercantiles derivadas del comercio electrónico.

De igual forma, a pesar de que es identificable la competencia jurídica de cada una de las Instituciones y organismos señalados, éstos han cooperado con la Asociación Mexicana de Internet, CONCANACO, PROMEXICO, con el IFT, la ANTAD, de la mano de la SE para fomentar el comercio electrónico; en virtud de lo anterior, se ha llegado a la conclusión del proyecto de norma mexicana que contempla principalmente un mecanismo de autorregulación el cual se da la flexibilidad de ser de ser de carácter voluntario para su aplicación.

La Norma Mexicana PROY-NMX-COE-001-SCFI-2018 se encuentra desde el mes de octubre del año 2018 en consulta pública para poder evaluar el contenido de la información y para que en el término establecido por la ley se presenten los comentarios con respecto al mismo. Sin embargo, se considera que esta normativa será un reto grande para las PyMes toda vez que, al ser una norma de aplicación voluntaria, si las PyMes no conocen desde un inicio dicha normativa o no cuentan con los elementos idóneos para acatar las disposiciones que señala, no tomarán en cuenta su contenido ni recomendaciones, por lo que en consecuencia podrían estar omitiendo su aplicación.

La normativa mencionada es resultado de los cada vez más reiterados casos de fraude cibernético a los que se enfrenta el comercio electrónico en México, "incremento de quejas de comercio electrónico en CONDUSEF de 2012, que eran 40,000 quejas anuales, a 1.7 millones en el primer trimestre de 2018"[167]: Lo anterior hizo que grandes entes de gobierno como CONSUSEF impulsarán dicha

[167] Vélez Medici, Armando "Nueva norma amenza al 95% del e-commerce en México", *Theemag*, Ciudad de México, agosto 2018, *https://www.the-emag.com/blog/nueva-norma-amenaza-el-95-del-e-commerce-en-m%C3%A9xico.*

normativa, sin embargo, se han llegado a identificar los principales problemas derivados de la emisión de dicha normativa.

La norma de comercio electrónico "busca exigir a los comercios en línea contar con mecanismos de autenticación de usuarios y resguardo de tarjetas, cuyo costo para tener esta certificación pudiera llegar hasta la ridícula cantidad de $50,000 USD anuales en una certificación de PCI *Compliance*"[168], se ha llegado a afirmar que el hacer que obligatorio el cumplimiento de la normativa a las PyMEs, únicamente estaría provocando la salida de la industria del *e-commerce*, toda vez que una PyME emprendedora no se encuentra en primeros términos con posibilidad para cumplir con las certificaciones y con los conocimientos técnicos que se les solicitan de primer plano, lo que haría que únicamente empresas transnacionales o nacionales con impotente presencia dentro del país, sean las que lleguen a cumplir con dicho ordenamiento.

Se ha llegado también se ha deducir que el imponer la carga directa a los responsables del *e-commerce* de un problema que le incumbe directamente a los bancos como lo es el fraude de tarjetas electrónicas, clonación, robo de identidad y robo de claves, es algo que queda fuera de la normativa planteada, por lo que puede inferirse que se está lejos de poder contar con una normativa que realmente apoye al comercio electrónico en México, hablando en el más amplio sentido de la palabra, ya que debe de considerarse a cualquier persona que realice transacciones en línea, no solo a aquellos que cuenten con la infraestructura y el capital económico para mantener un comercio a través de medios electrónicos.

4.2. El comercio internacional electrónico en México

México, a pesar de haber entrado dentro de la era digital recientemente, ha incursionado a ella de manera acelerada, tratando de posicionarse dentro de una época moderna de las comunicaciones, la cual ha hecho con la ayuda de empresas tanto públicas como privadas para llegar a tal fin.

[168] *Idem*

Remontándonos a los orígenes que dieron lugar a la incursión del Internet en México, tal y como lo expone Nava González y Breceda Pérez, "México logró establecer de manera formal el primer enlace con Internet a través del Instituto Tecnológico de Estudios Superiores de Monterrey, en el año de 1989, siendo así el primero país latinoamericano en conectarse a la red"[169],posteriormente se encontró con problemas relativas a la restricción de realizar actividades comerciales en línea, disposición impuesta por los Estados Unidos, y aunque en 1992 fue eliminada esta disposición, hasta el año de 1994 México realizó la primera transacción electrónica y comenzó a realizar comercio electrónico.

A pesar de ser una práctica relativamente joven para el estado mexicano, éste ha sabido incursionar en ella y en la medida de sus posibilidades entrar al mundo digital y al comercio electrónico, esto, como una nueva forma de crear relaciones sociales y comerciales.

En el año 2000, a pocos años de haberse implementado en México el comercio electrónico, había pocas esperanzas de que fuera una buena práctica su adhesión a la vida diaria desde un punto de vista comercial, sabían los resultados que estaban arrojando a los demás países Europeos y en Estados Unidos, pero no estaban familiarizados de cómo llevarlos a cabo, los empresarios y organismos mexicanos no lograban identificar qué era necesario implementar para poder llevarlo a cabo de una manera práctica y funcional.

"La tesis principal de esta etapa era la idea de difundir la imagen y las características más importantes de una empresa entre el cada vez más numeroso público de Internet, especialmente del web. El mecanismo para lograr esto: tener una página web"[170]. Sin embargo, la poca experiencia que experimentaba México con respecto a estos temas, hacía más difícil la adecuada implementación de una página web que pudiera solucionar un problema en específico y brindar un crecimiento comercial adecuado. "Como el énfasis estaba en tener una página y

[169] Nava González, Wendolyne y Breceda Pérez, Jorge Antonio, *México en el contexto internacional de solución de controversias en línea de comercio electrónico,* México, UNAM, 2017, p.1.

[170] Guardia, Carlos de la, "La evolución del comercio electrónico", *Razón y palabra*, México, 2000, núm. 20, *http://www.razonypalabra.org.mx/anteriores/n20/20_cguardia.html.*

no necesariamente qué poner en ella, las empresas se conformaban con volcar información contenida en folletos y otras publicaciones organizacionales ya existentes, como recortes de prensa y propaganda publicitaria".[171]

A pesar de esta reflexión desfasada que tenían los organismos públicos y empresas mexicanas, sabían que era necesario comenzar a implementar el uso de los medios digitales para empezar a posicionarse en la era digital y competir directamente con los organismos comerciales considerados de primer mundo; comenzaron a considerar que así como alguna vez fue un lujo el contar con energía eléctrica o servicios de telefonía, hoy en día se consideraba una necesidad de primera mano, el caso del Internet no era la excepción, se transformaría en una necesidad de comunicación.

Años más tarde, el comercio electrónico en México fue posicionándose dentro del mercado global, sin embargo, no ha mostrado todo su potencial. Para el 2014 se lograba ver un cambio dentro de la expectativas para generar comercio electrónico en México, se han llegado a pronosticar estadísticas favorables para el posicionamiento del comercio electrónico, sin embargo, este crecimiento no logra concretarse completamente, principalmente por la desconfianza que experimentaban los usuarios; simple y sencillamente los usuarios no apostaban por utilizar servicios de la banca o compra el línea, por temor a ser víctima de un fraude o que el producto no llegue a sus manos.

En el año 2016, se identificaron otros factores que van más allá de pertenecer únicamente a la era digital para poder formar parte del *comercio electrónico.*

Estudios formulados han demostrado que los sitios que tienen más posibilidades de permanecer dentro de la competencia que exige el comercio electrónico, como lo son en las ventas y en permanecer por más tiempo a disposición del público, son los que cuentan con plataformas seguras de pago.

"Cifras presentadas por PayPal, dan a conocer el panorama de crecimiento para el comercio electrónico en México, sobre todo en el segmento de Pymes, y es que, al

[171] *Idem.*

parecer, es el sector que más crece en este rubro"[172].

Con el paso de los años, de conformidad con lo señalado por la Asociación Mexicana de Internet, en el año 2016 "El comercio electrónico en México tuvo un crecimiento anual de 59% con lo que superó los 257,000 millones de pesos de ventas en el año[173], Sin embargo, la misma asociación reconoce que aún hay grandes desafíos que atacar, tal es el caso de la implementación de servicios financieros y el acceso a las tecnologías.

Actualmente, en México varios especialistas en comercio electrónico han señalado que los consumidores mexicanos que adquieren productos en línea, es decir, a través del comercio electrónico, prefieren realizar las búsquedas de los principales productos a adquirir a través de la plataforma de *Google* y pocas veces lo hacen en la búsqueda directa de las tiendas en línea.

De igual forma, se ha podido observar con el paso de los años que el comercio electrónico ha llegado para comenzar a quedarse en la mejora de relaciones interpersonales, que hace que se provoquen avances significativos en el estilo de vida de la sociedad, optimizando tiempos y dinero, tal y como lo señala Doris Oropeza "los consumidores tienen ventajas, como evitar costos de desplazamiento, una mayor oferta de productos o servicios, costos menores de ciertos productos en comparación con el mercado físico"[174]

También se observan una serie de mejoras para las empresas que comercializan los productos o servicios, gracias a la aparición del comercio electrónico "las empresas encuentran menores barreras en el mercado, una mayor cantidad de clientes potenciales y, en muchos casos, reducción de costos en el establecimiento de la empresa, pues muchas de ellas no necesitan un espacio de venta al cliente presencial"[175]

Se han realizado importantes estudios de los medios que los usuarios o

---

[172] Baez, Javier, "El comercio electrónico en México en 10 pasos", *Dinero en Imagen*, *http://www.dineroenimagen.com/2015-04-14/53963.*

[173] "El estado del comercio electrónico en México", *El Economista*, 18 de noviembre de 2016, https://www.eleconomista.com.mx/arteseideas/El-estado-del-comercio-electronico-en-Mexico-20161118-0169.html

[174] Oropeza, Doris, *op cit*, p. 3.

[175] *Idem*.

compradores en línea normalmente utilizan para realizar sus compras en línea a través de Internet, creándose varias listas, una de las principales creadas por *ComScore*[176], donde señala las principales posiciones de los sitios que más visitas virtuales tienen en México, obteniendo el primer lugar Mercado libre, seguidas por marcas como *Liverpool, Wal-Mart y Amazon*.

El comportamiento que tienen los usuarios y que demuestran cuáles son sus principales necesidades a la hora de realizar una compra en línea, afirmándose que "un 58 por ciento realiza búsquedas relacionadas con algún producto que buscan, mientras que un 27 por ciento va más allá y busca comentarios acerca de los productos"[177]. De igual forma, México se ha posicionado como uno de los principales países con mayor atracción al comercio de lujo "en México este mercado es considerado tan atractivo: por la cantidad de jóvenes que habitan aquí y, sobre todo por ser valorado como un país de estratos altos con gran concentración de la riqueza"[178]

Asimismo, señala que los usuarios en su mayoría primero *googlean*[179] el artículo que desean adquirir antes de decidirse si desean comprar alguno o no, razón por la cual solo un tres por ciento va directamente al portal de compra en línea del producto.

Las principales fallas que hacen que el comprador en línea desista de completar una compra, son las siguientes:

- Mala información proporcionada en los sitios web.
- Fallas tecnológicas en el sitio.
- Miedo de los usuarios de que la página no sea segura y que sean expuestos a algún tipo de estafa en la red.
- Por mala información de precios.

---

[176] Proveedor de servicios de medición de audiencias, la cual utiliza una metodología informática que permite registrar todos los visitantes de un sitio web y arroja un resultado aproximado del número y calidad de la audiencia evaluada.

[177] Venegas, Eduardo, "Las cosas que los consumidores aman y odian de comprar online", *Revista Merca 2.0*, México, 22 de mayo 2017, *https://www.merca20.com/las-cosas-que-los-consumidores-aman-y-odian-de-comprar-online/.*

[178] Camacho Rodríguez, Karla Teresa, *op. cit*., p. 72.

[179] Término utilizado para referirse a la búsqueda que los usuarios realizan de manera habitual en la plataforma de internet denominada "Google".

- Por una mala atención recibida en línea.
- Por malos comentarios que otros usuarios dejan en las páginas web y que hacen que se tenga una mala impresión del producto.
- Por entrar a una página de web y que ésta se encuentre rodeada de publicidad que no es eficiente o que entorpece la visibilidad de la página o navegación.
- Porque se tiene incertidumbre del destino y uso final de los datos personales proporcionados al momento de realizar una compra en línea.

Por otro lado, el 21 por ciento de los usuarios señaló que las principales razones por las que siguen sin confiar en el comercio electrónico son[180]:

- Búsquedas de productos agotados o que no se encuentran disponibles en el mercado.
- La dificultad técnica de las páginas que no permite tener una visibilidad y manejo adecuado de la página.

De lo anterior, se deduce que el conocer la posición en la que se encuentra el comercio electrónico y saber cuáles son las principales deficiencias que tiene, es información clave para poder atacar los problemas del despegue nacional del comercio electrónico, es decir, es necesario conocer las necesidades de los ciberconsumidores; sin embargo, conocer las deficiencias no es suficiente, si no se cuenta con un plan de acción que obligue a todos los proveedores de bienes y servicios a acatarlos o establecer lineamientos para mejorarlos, solo así podrá visualizarse un avance generalizado.

Sin duda con estas cifras se ha podido apreciar, el crecimiento que día con día genera el comercio electrónico en México, el cual, aunque no es una cifra que se iguale a las de otros países del mundo en ninguna forma, se visualiza claramente que comienza a emplearse el comercio electrónico por los usuarios de Internet, quienes diariamente descubren las ventajas de su uso y lo implementan a sus actividades cotidianas.

[180] Venegas, Eduardo, *op. cit*.

4.3. El tratamiento de datos personales por empresas transnacionales que operan en México

Varias de las grandes trasnacionales que operan en México a través de alguna filial, están comenzando a realizar cambios considerables dentro de sus políticas de privacidad y seguridad de la información; sin embargo esto es algo que se ha comenzado a dar de manera paulatina, y principalmente con aquellas empresas que tienen gran actividad en el mercado europeo.

La aparición de las tecnologías de la información dio pauta para que las empresas comenzaran a identificar la necesidad de crear sistemas de protección de información, aunque es conocido que la regulación europea en temas de seguridad de información es avanzada, Latinoamérica ha dado también muestra del trabajo que ha comenzado a desarrollar al respecto y sobretodo se puede visualizar la cooperación privada para proteger este tipo de temas, quienes en la mayoría de las ocasiones, se basan en la ética y la autorregulación, para encargarse de temas en años anteriores no estaban completamente regulados por el derecho, tal es el caso de la protección de datos personales por las empresas dedicadas al comercio electrónico transnacional, ya que pudiera entenderse que una vez que sale la protección de información de la esfera de jurisdicción de un determinado lugar, las empresas responsabilidad no tienen alguna de ofrecer medidas de seguridad de la información de recaban y tratan.

Tal y como señala Colmenarejo Fernández “las estructuras sociales que comienzan a manifestarse a través de la gestión, disponibilidad y uso de las Big Data, hacen emerger conflictos éticos en muchos casos heredados de la ética de los negocios, aunque ahora éste se vea superada por las circunstancias que las que operan la generación y gestión masiva de datos”[181]. Para la autora la labor de recolección de información que realizan las empresas, requiere de un gran esfuerzo de poder contribuir en la salvaguarda de información a través de la ética

[181] Colmenarejo Fernández, Rosa, *Una ética para Big data: introducción a la gestión ética de datos masivos*, Barcelona, UOC, 2018, p. 12.

empresarial y sobre todo ve a la ética aplicada al Internet"[182] de las cosas cómo una forma imprescindible para proteger la información.

4.4. El tratamiento de datos personales por micros, pequeñas y medianas empresas

Con respecto al sector comercial en línea, es importante considerar que la gran mayoría de los *e-commerce* mexicanos constituidos por MiPyMes dedicados a la venta en línea al mercado europeo aún es poca. Los MiPyMes que podrían llegar a considerarse como vendedores directos de la UE, son las agencias de viajes, artículos para el hogar y artesanías, por mencionar algunos ejemplos.

México está consciente del retraso de actividades de comercio electrónico que tiene en consideración con otros países del mundo, por lo que, ha realizado campañas a través de organismos gubernamentales tales como Proméxico*[183]*, para capacitar a las empresas mexicanas en el ámbito del *e-commerce[184]*. La intención principal de incentivar este tipo de prácticas comerciales es la de promover el comercio nacional hacia el extranjero, y como forma de llegar a ese objetivo, prevé ofrecer las herramientas técnicas y el conocimiento económico y legal que necesitan las empresas para alentar el *e-commerce,* principalmente en Asía y Europa.

Tomando en consideración los principales objetivos del RGPD, desde su perspectiva de proteger la información de cualquier persona en toda su Unión y para este caso en específico, que tenga el estatus de *ciberconsumidor,* establece que se creó el Reglamento para evitar divergencias que dificulten la libre

[182] Para la autora la ética aplicada al internet de las cosas puede considerarse una ética de ámbito profesional, toda vez que se ocupa principalmente de lo que señale un determinado grupo de expertos, sin embargo considera necesaria la ética empresarial para que dichos expertos que trabajan en el sector público y privado colaboren para desarrollar en común una cultura ética que permita tomar decisiones orientadas a una sociedad o sector.

[183]Pro México es una institución gubernamental que se encarga de promover la atracción de inversión extranjera directa hacia México para exportaciones de productos o servicios, así como la internacionalización de las empresas mexicanas para contribuir a través de la importación con el desarrollo económico y social del país.

[184]*https://www.gob.mx/promexico/articulos/aprende-a-exportar-a-traves-de-internet*

circulación de datos dentro del mercado interior, por lo que es necesario que se proporcionen seguridad jurídica y transparencia las microempresas y las pequeñas y medianas empresas.

Las MiPyMes deberán de ofrecer a todas las personas físicas de cualquier Estado miembro que conforme la UE, el mismo nivel de derechos y obligaciones exigibles, así mismo serán extensibles estas obligaciones a los responsables y encargados del tratamiento, cuando sus actividades económicas y números considerables de datos en tratamiento lo ameriten.

De igual forma, tomando en consideración la desventaja que tienen las MiPyMEs frente a las empresas multinacionales y trasnacionales, el RGPD ha establecido una serie de excepciones que son de aplicación directa para aquellos comercios que cuenten con menos de 250 empleados.

Es importante considerar el concepto que tiene el RGPD, con respecto a la figura de empresa. De acuerdo con el artículo 4º del reglamento, será considerado como “empresa: a la persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñan regularmente una actividad económica”.

En virtud de lo anterior, no deberá subestimarse el carácter con el que se ostenta un vendedor en línea, como se pudo observar el capítulo segundo de este trabajo de investigación, de acuerdo con el CCo, nuestro país reconoce la actividad de comerciante a toda aquella persona que realice actividades mercantiles; así mismo, a manera de reafirmación, el RGPD establece claramente la responsabilidad de cualquier persona que se dedique a una actividad comercial a través de medios electrónicos, por lo que será aplicable cualquier disposición que señala el reglamento con respecto a la protección y tratamiento de datos.

4.5. Los problemas de aplicación de la normativa interna para protección de datos personales a los actos realizados a través del e-commerce en México

Primeramente, es importante valorar el avance tecnológico y legislativo que otros países, principalmente los constituidos dentro de la UE, tienen en comparación con la posición que actualmente cuenta México en el mercado digital, el uso de las TICs, el nacimiento del *e-commerce* y sobre todo la legislación en temas de protección de datos personales, cuentan con un avance significativo en tiempo y espacio, que deja en considerable desproporción a México desde el punto de vista del ámbito de operación; sin embargo, esto no ha hecho que México quede completamente desfasado, actualmente se trabajan en diferentes aspectos que tratan de posicionar la protección de información dentro del comercio electrónico, de acuerdo con las exigencias que marca el ámbito internacional.

4.5.1. Avances actuales en la materia

En la actualidad el desarrollo de las TICs y la repercusión que éstas han tenido dentro de la economía digital han permitido que conocer la importancia que tiene la información en cualquiera de los sectores en que una empresa tiene presencia.

Por su parte, la creación de normativas nacionales como la LFPDPPP han permitido que se establezcan las bases de la protección de datos personales y la divulgación de sus contenido por parte del sector privado empresarial, para que éstos tengan conocimiento de cómo deberán de tratar y cuidar la información que poseen como resultado de sus actividades económicas, avocándonos directamente en nuestro tema de estudio, a través de las actividades de comercio electrónico trasnacional.

La protección de datos personales tiene un avance significativo tanto en su Ley vigente en México como en su Reglamento, se tienen contemplados los derechos ARCO y la confidencialidad de la información. Tal y como lo señala Mendoza Enríquez:

> Los datos personales, en posesión de las empresas, abarcan dos vertientes: por un lado, la responsabilidad de guardar confidencialidad de los datos personales a su cargo, así como solicitar el consentimiento de los titulares, en caso de envío o cesión de información; por otro lado, el derecho que

> tienen los titulares de datos personales, para ejercitar sus derechos de acceso, rectificación, cancelación u oposición de datos personales (derechos ARCO)[185]

Como resultado de la anterior aseveración, puede apreciarse que la LFPDPPP vigente abarca dicha disposición y sobretodo maneja los principios que toda empresa deberá de tener para establecer un adecuado cumplimiento de protección de datos[186].

1. Principio de licitud. Toda empresa tendrá que usar medios lícitos para obtener la información y deberá de comunicarlo de una manera clara y no fraudulenta.
2. Principio de finalidad. Cualquier tratamiento de datos personales deberá de estar plenamente justificado y coincidir con las finalidades para lo cual fue recolectada la información.
3. Principio de lealtad. La empresa deberá de tratar los datos personales siempre con el más alto estándar de confidencialidad y deberá de cuidar la información de acuerdo con las disposiciones que enuncie la ley.
4. Principio de consentimiento. Este principio señala que las empresas solo deberán de utilizar la información una vez que cuenten con el consentimiento de autorización por parte de los titulares de la información, sin embargo, tal y como se mencionó en líneas anteriores dentro de la presente investigación, este principio cuenta con debilidades, ya que permite el consentimiento tácito, una vez que el titular no se oponga al tratamiento de la información.
5. Principio de proporcionalidad. Este principio señala que la empresa únicamente podrá utilizar la información en relación con el cumplimiento de las finalidades que notifica a través de sus avisos de privacidad, y en proporción a las finalidades de su tratamiento.
6. Principio de información. Este principio es de información principalmente, toda vez que la empresa tiene la obligación de informar

[185] Mendoza Enríquez, Olivia Andrea, "Marco jurídico de la protección de datos personales en las empresas de servicios establecidos en México: desafíos y cumplimientos, *Revista IUS*, Puebla, vol.12, núm. 41, ene- 2018.
[186] *Idem.*

en todo momento a los titulares de la información, la forma en la que están siendo tratados sus datos personales y las finalidades para los que son empleados los mismos.

7. Principio de responsabilidad. El responsable de la información será el obligado principal de velar por el buen uso y cuidado de los datos personales que le han sido encomendados, evitando en todo momento que caigan en manos de terceros no autorizados.

4.5.2. Retos actuales

El reciente desarrollo tecnológico ha hecho que se revolucione la forma en la que se regula el derecho empresarial, las nuevas normatividades han hecho que las empresas no queden exentas del cumplimiento de ciertas normas que imponen las prácticas comerciales que realizan; la protección de la información se ha vuelto una de las más importantes para ese sector.

Tal y como señala Mendoza Enríquez "factores como el uso indebido de la información o la vulneración de medidas de seguridad de la misma, ponen en riesgo la reputación de las empresas, y las podrían hacer acreedoras de sanciones, por lo que resulta necesario estudiar el tema desde una perspectiva regulatoria, que incluya: legislación, normas sectoriales y buenas prácticas"[187], es decir, es imprescindible que el sector empresarial comience a implementar en sus reglamentos internos el rubro dedicado específicamente a la protección de la información que tienen en su poder, no solo de manera consensual, sino, obligatoria.

Aunque el desarrollo tecnológico ha hecho que sean facilitadas infinidad de tareas reduciendo costos y tiempos, también debe de considerarse el factor indirecto que se ha provocado a través de estas nuevas herramientas de la información, es importante considerar que las tecnologías "también han propiciado

[187] Mendoza Enríquez, Olivia, *op. cit.*

una serie de desafíos en torno a la seguridad de la información, la protección de los datos personales y el cumplimiento de la regulación en la materia"[188].

En virtud de lo anterior, es necesario conocer primero, cuál es la posición empresarial frente al tratamiento de la información, para clasificar las principales utilidades por la recolección de información y su tratamiento y determinar los principales desafíos que cada organización debe de considerar para cumplir con el debido cumplimiento de la noma, por lo que, tal y como señala la autora Mendoza Enríquez

> …para dimensionar la importancia que ha cobrado el derecho de la protección de datos personales, es necesario hablar del valor económico y social de la información al interior de las organizaciones. Esto debido a que la reputación y modelo de negocio de una empresa están basados en la confianza, estándares de protección de datos personales y medidas de seguridad de la información que se implementen[189]

A través de la presente investigación se han citado ejemplos de grandes empresas transnacionales que su principal actividad es la recolección de la información y sus principales activos dependen de ese tratamiento de información "Hemos visto que empresas globales, como *Google* o *Facebook*, basan su modelo de negocio en la información de las personas. Más allá de la discusión sobre si es legal y legítima esta práctica, podemos aseverar que el desarrollo tecnológico ha permitido recabar, almacenar y procesar grandes cúmulos de información en tiempo real, lo cual, le ha dado un valor agregado a la información"[190]

Por lo anterior, es necesario que las empresas más allá de una buena práctica de protección de información de manera libre, se sujeten a una normatividad que impongan estándares especiales para el tratamiento y protección de toda aquella información que diariamente recolectan en servidores y tratan de manera muchas veces arbitraria. No debe de darse por sentado el valor económico de cierta información, ni estimarse un valor determinado por la misma; por lo que, si las empresas no determinan la forma en la que deben proteger la información, podrían estar vulnerando información si no la tratan debidamente.

---

[188] *Idem*
[189] *Idem*
[190] *Idem*

Aún es necesario prestar atención a temas de protección de información. El tema de la seguridad en la información es un tema delicado, partiendo de la premisa de que todo el desarrollo tecnológico que están experimentando las empresas de manera inconsciente, ha provocado que no se atienda de manera responsable, el uso, almacenamiento y protección de toda la información que sustenta su operación. Diversos autores como Astudillo Catalina y otros, señalan al respecto:

> Las empresas están obligadas a anticiparse a los diversos escenarios de riesgo de información, debido a una vertiginosa evolución de la informática, el constante cambio tecnológico, y el rápido crecimiento de las múltiples transacciones de negocio, en los cuales la información y los dispositivos computacionales están inmersos en escenarios como ataques de hackers, usuarios del sistema, amenazas lógicas, y una gran variedad adicional.
> Sin embargo, debido a la falta de conocimiento sobre cómo protegerla adecuadamente o a la complejidad exigida por muchas normas internacionales y mejores prácticas de desarrollo, múltiples organizaciones descuidan asegurarla[191]

En consecuencia, se han llegado a crear nuevas metodologías que permitan que las empresas implementen una mejor labor de seguridad de la toda la información que almacenan, a esta técnica la han denominado *pentesting*.

El *pentesting*, es práctica ha sido implementada en algunas empresas que de primer momento, lo han hecho con fines experimentales, que les permitan medir el nivel de seguridad con que hasta ese momento cuentan, y atacar todos los puntos vulnerables que tengan hasta ese momento.

Se ha definido al *pentesting* como "una de las técnicas de evaluación que apoyan al análisis de brechas de seguridad, análisis que debe ser realizado por una persona con conocimientos técnicos, pero con principios éticos"[192].

Se considera a la deontología informativa como una de las principales características que debe de tener la persona que realicen estas prácticas, toda vez que será la única forma en la que podrá separarse de una confusión de investigaciones informáticas con fines delictivos. Esta "característica diferencia a

[191] Astudillo, Catalina *et al*, "Acometer contra un ERP con Software Libre", *Enfoque UTE*, vol.9, núm.1, Marzo 2018, p. 139, *http://ingenieria.ute.edu.ec/enfoqueute/*
[192] *Idem*

un atacante común, conocido en esta época como un “hacker de sombrero negro”, que es una persona que irrumpe la seguridad de la organización con el fin de beneficiarse de la información en ella almacenada”[193]

El *pentesting* marca la siguiente metodología:

1. El método utilizado;
2. La conceptualización del escenario de pruebas;
3. La definición del laboratorio de pruebas;
4. Los resultados obtenidos en las diversas fases del pentesting;
5. Las conclusiones obtenidas en las pruebas de evaluación a una aplicación desarrollada en Oracle APEX 5;

Dentro de los beneficios que se sugieren se obtendrán de la implementación de los *pentesting*, están los siguientes:

1. Mantener un punto de equilibrio entre la funcionalidad y la seguridad, toda vez que se en muchas ocasiones las prácticas de aseguramiento de información en plataformas y aplicaciones no solamente por el tipo de tecnología que se utiliza para su aseguramiento y resguardo, sino que también es importante considerar que tan funcional y práctico es su uso.
2. El filtrar los datos de entrada reducirá el riesgo de contar con información errónea en la plataforma.
3. La importancia del cifrado de datos es inminente. Lo anterior, para que se asegure de manera adicional el fácil acceso al conocimiento de la información, que su envío, transmisión y recepción, en caso de ser vulnerado, se encuentre con una mayor seguridad y candados al momento de que otro sujeto no autorizado quiera acceder a ella de manera fácil, rápida e ilícita.
4. Es necesaria laadopción de certificados digitales que validen, no solo el sitio web sino además la organización.

[193] *Ibidem*, p. 140.

Las herramientas VEGA, OWASP ZAP, han revelado el uso de los métodos GET, POST, PUT, DELETE provistos por un sistema web para el acceso a la información. De los anteriores, los dos últimos deben ser manejados con cautela, pues PUT permite cargar contenidos y DELETE eliminarlos. Estos métodos deben ser analizados y evaluados antes de su puesta en producción[194].

4.5.3. Brechas y obstáculos a superar

Se considera que a pesar de lo estricto e inflexible que puede mostrarse el RGPD algunas empresas transnacionales con presencia en México ya han comenzado a implementar sus prácticas de regulación, toda vez que desean en primeros términos cumplir con una ley que obligatoriamente tienen que observar, pero sobretodo desean generar confianza de compras en sus clientes.

Por otro lado, existen empresas que simplemente no consideran necesaria la implementación en México, o aún con conocimiento no estiman necesaria la inversión en temas de protección de datos, pues es una inversión que de primer momento no generará ganancias inmediatas y cuentan con otro tipo de prioridades a corto o mediano plazo.

Sin embargo, más allá de considerar si esa inversión será o no redituable, debe de tenerse en cuenta que a largo plazo y con el crecimiento de un mercado digital,hará que la normativa comience a tener aplicación absoluta, por lo que en un futuro, las sanciones por incumplimiento comenzarán a tener presencia en México, si no se toman medidas preventivas a corto plazo.

Por otro lado existe otro sector empresarial en que reconoce que tiene que cumplir con ciertos estándares de seguridad, realiza actos de protección al respecto, sin embargo desconocen el verdadero alcance de los servicios que contratan en materia de protección de información y viven bajo el error de que están completamente deslindados de responsabilidades, es importante mencionar que lo anterior no es así. Algunos de los casos más frecuentes son los siguientes:

[194] *Ibidem,* p.147.

a) Consideran que subcontratando los servicios de alojamiento de datos, se transfieren completamente las obligaciones al tercero que está tratando los datos personales. En primer término deberá de revisarse detalladamente el nivel de responsabilidades tanto del proveedor de servicios de alojamiento como de la empresa contratante, a través de contratos de prestación de servicios que señalen la figura de responsable y encargado de tratamiento que manifiesta la propia LFPDPPP y su Reglamento. Si se establece claramente en los contratos respectivos y avisos de privacidad respectivos, las empresas podrán estar libres de preocupaciones, caso contrario podría existir un grado considerable de responsabilidad compartida, por no establecer adecuadamente las obligaciones de cada una de las partes.
b) El sitio web de *e-commerce* permite tanto el pago en línea a través del sitio web como el pago telefónico, sin embargo se subcontrata el servicio de banca en línea, pero se realiza de manera personal por la empresa el monitoreo y compras a través de líneas telefónicas. En tal supuesto, la responsabilidad será completamente de la empresa, toda vez que, como ya se ha hecho alusión en el capítulo primero de la presente investigación, el comercio electrónico se hace a través de cualquier medio óptico, magnético o con cualquier otra tecnología, y al aceptar recibir datos personales a través de líneas telefónicas que son completa responsabilidad de la empresa, la empresa deberá responder ante cualquier vulneración.
c) Cuando la empresa construye de cero la página web y debido a que es una empresa con un flujo de información mínimo, considera que éste puede mantener y proteger los datos personales de las transacciones que se realicen. Lo anterior, es una práctica común entre los micros, pequeños, e incluso medianas empresas, quienes confían en que de manera manual podrán llevar a cabo el control y tratamiento de la información, sin embargo, una vez que el negocio comienza a crecer en

número de clientes, se vuelve un caso imposible de proteger de manera rápida y eficiente.

De los tres puntos expuestos, se considera que el más vulnerable de incidir en algún incumplimiento es el último, toda vez que el cumplimiento del RGPD por parte de las micro, pequeñas y medianas empresas puede observarse que es un reto, pues con mucha frecuencia subestiman el costo beneficio de contar con un sistema adecuado de protección por lo que prefieren realizar el cumplimiento de la información de manera manual, no es intención con de menospreciar la intención que realizarán las MiPyMEs; sin embargo, se predice, que si el negocio comienza a crecer, será difícil de que los propios administradores de la empresa, se dediquen exclusivamente al tratamiento de los datos personales que se establezcan.

Es importante hacer notar que no puede juzgarse completamente la mala administración de un *e-commerce* por el simple desconocimiento de la ley, sino que también deben de considerarse otros factores que incluso trastocan fondos sociales, culturales y tecnológicos, la transición de una era digital ha hecho que las empresas que toda su vida se han dedicado al comercio, se enfrenten a nuevos retos aún desconocidos para ellos, que van más allá de conocer el mercado al cual se enfocan a través de sus productos, por lo que se considera fuertemente que los empresarios comiencen a inmiscuirse en temas actuales que permitan comprender y facilitar la aplicación de las normativas que han surgido en las últimas décadas con respecto al comercio y especialmente con respecto al comercio electrónico.

4.6. Alternativas para un adecuado cumplimiento a la protección de información de carácter personal del e-commerce en México a través de las tecnologías de la Información

Actualmente, es prácticamente una locura concebir las relaciones humanas sin la tecnología, algunas de las ventajas que ha traído consigo las tecnologías es el hacer la vida de cada uno de personas más fácil y rápida, por lo que al día de hoy se encuentran dentro de nuestras actividades cotidianas de alguna u otra forma, las comunicaciones, el aprendizaje, la investigación, las relaciones interpersonales, las relaciones gubernamentales, la economía y claro está, la forma en que se realizan transacciones comerciales, son solo algunas de las muchas actividades que han evolucionado con la aparición de las tecnologías.

Las tecnologías de la información nacen de la rama de la informática, en la cual, se ha llegado a señalar que desde el punto de vista gramatical:

> El término informática proviene del francés *informatique* y está formado por la contracción de las palabras *information* y *automatique*. Este término fue aceptado en el resto del mundo. Existen muchas definiciones posibles de informática. La Academia Francesa de la Lengua la define en 1966 como: la ciencia del tratamiento racional, por medio de máquinas automáticas de la información, considerada como un soporte de los conocimientos humanos y de las comunicaciones en los campos técnicos, económicos y sociales[195].

Como puede observarse, el término deriva de la información, es decir, del acumulado de conocimientos que una persona o ente puede generar a lo largo de su vida o para un fin específico, sin embargo, para definir lo que puede considerarse como el término propio dicho de informática y su finalidad, es importante considerar lo que señalan Corona Cabrera quienes afirman que:

> …es una disciplina relativamente nueva que tiene lazos con la ingeniería, las matemáticas y los negocios, pero tiende a centrarse más en el proceso de cálculo que en el hardware de la máquina; por ello, la informática es considerada como la ciencia de la información para la mayoría de los autores, pero muchos informáticos prefieren referirse a la informática como la ciencia de la computación[196]

[195] Corona Cabrera, Alfredo *et al*, *Tecnologías de la información y comunicación*, México, UNAM, 2012, p.22.
[196] *Ibidem*, p. 23.

Es importante considerar que, aunque se conciban a las tecnologías de la información como unas herramientas de comunicación relativamente recientes, no debe de confundirse que más allá de considerarlas como actuales, deben de ser consideradas como evolutivas, ya que de éstas son cualquier forma de comunicación a través de medios informáticos, se ha llegado a considerar que las primeras TICs fueron los el telégrafo, el teléfono, la imprenta, la radio y la televisión[197], solo por mencionar algunos; es decir, las tecnologías que al día de hoy se consideran, tal es el caso del Internet, aplicaciones, teléfonos móviles, bandas electromagnéticas y códigos de barras, no deben considerárseles como los primeros, deberán de considerarse como sucesores tecnológicos.

Por su parte, las TICs han podido establecerse como una rama de la informática que dentro de sus principales características se encuentran la innovación y el desarrollo de sistemas que agilizan la realización de determinadas tareas.

Para Riasco las TICs son "el conjunto de sistemas y productos que captan la información del entorno, la almacena, la procesan, la comunican, y la hacen inteligible a las personas, así como la transmisión de la misma a través de la interconexión de equipos que facilitan la construcción de redes"[198]

Por su parte, autores como Galvez, De Lerma y García señalan que las TICs están "constituidas por inversiones de la empresa ha realizado en equipos de computación, software y medios de comunicación"[199]

Así mismo, se ha llegado a afirmar por Almansa y Castillo, las TICs "constituyen unos de los medios más adecuados para aproximarse al entorno y desarrollar un profundo conocimiento sobre los diferentes agentes que lo

[197] *Ibidem*, p.24.

[198] Riascos, Erazo, *et al, Efectividad de las TIC en los procesos administrativos de las PYMES de Santiago de Cali*, Gerencia tecnológica informativa, vol. 14, 2015.

[199] Galvéz Albarrecín, Edgar, ***et al,*** *"*Tecnologías de información y comunicación, e innovación en las MIPYMES de Colombia", *Cuadernos de Administración*, vol. 30, núm. 51, enero-junio 2014, *http://www.redalyc.org/articulo.oa?id=225031330008.*

conforman. De ésta forma, actuando como una fuente de obtención y generación de información"[200]

Cabe señalar que el mejor representante de las tecnologías de la información es el Internet, "ningún medio de comunicación ha conseguido una penetración tan rápida como Internet. Su implementación ha repercutido en la sociedad en general y en la comunicación en particular"[201]

Para comprender mejor esta tecnología de la información se ha apoyado en algunas de las definiciones que se han construido para identificarla de una manera generalizada y clara, por lo que ha sido establecida como:

> Una red de computadoras a nivel mundial, una herramienta de comunicación con decenas de miles de redes de computadoras unidas por el protocolo TCP/IP. Ofrece distintos servicios, como el envío y recepción de correo electrónico (e-mail), la posibilidad de ver información en las páginas Web, de participar en foros de discusión (News), de enviar y recibir ficheros mediante FTP, de charlar en tiempo real mediante IRC[202]

Las TICs, y el Internet específicamente, han sido pieza clave para que pudiera desarrollarse el concepto de lo que ahora se conoce como comercio electrónico o *e-commerce*; Antes de contar con estas herramientas de comunicación e interacción se obligaba a que los consumidores de un producto en específico realizará la búsqueda de éstos en forma personal; en la cual acudía directamente al establecimiento para ver si se encontraba el artículo de su interés, o un artículo lo más parecido posible, gastando tiempo y dinero en tal búsqueda; ahora con la ayuda del comercio electrónico se le da acceso a que con un solo *click* en cuestión de segundos acceda a una base de datos que le permite escoger entre una gran cantidad de artículos que desean o en muchas ocasiones- que superan las expectativas de lo que en un inicio el consumidor busca. "lo cierto es que la tecnología redefinió las reglas de los mercados, planteando la posibilidad

[200] Almansa Martínez, Ana y Castillo Esparcía, Antonio, "Comunicación Institucional en España. Estudio del uso que los diputados españoles hacen de las TIC en sus relaciones con la ciudadanía", *Revista Latinoamericana de Comunicación*, Quito, núm. 126, 2014, pp. 23-30.
[201] *Ibidem*, p. 24.
[202] Corona Cabrera, Alfredo *et al, op. cit., pp. 42-43.*

que nuevos competidores aparezcan constantemente, a velocidades nunca antes observadas".[203]

Por lo anterior, el mercado global, principalmente las empresas internacionales, han comenzado a implementar el uso de las tecnologías para llegar a un mayor número de consumidores y lograr que sus activos crezcan significativamente, se ha identificado el sin fin de beneficios que trae consigo el uso de las tecnologías de la información. Se ha llegado a afirmar que las "Tecnologías de la información hacen posible un mayor trabajo en red, que pone la información suficiente y oportuna para tomar decisiones y responder a las exigencias del mercado"[204]

Así mismo se ha reconocido la importancia de las tecnologías de la información como parte fundamental para el desarrollo de cualquier empresa actual, y en su caso, reconocer el doble mérito que tienen para las empresas dedicadas de manera exclusiva al *e-commerce,* "el avance en las TIC han dado un paso a un nuevo género de oportunidades de negocio y de este modo ampliar el horizonte de las empresas a explorar nuevos modelos de negocio. Este nuevo siglo presenta una fuerte propulsión para que las empresas adopten estas tecnologías (como el Internet) como medio para una nueva conducta empresarial"[205]

En virtud de lo anterior, se destaca que es importante como sociedad comenzar a aprovechar todas las herramientas que las mismas tecnologías de la información nos ofrece, para poder brindar seguridad jurídica a todas las personas que hacen uso del Internet, y que así se proteja uno de los derechos humanos fundamentales de toda persona en México como lo es su privacidad; toda vez que "se pretende que el Estado logre que la industria de las redes sociales se

[203] Gariboldi Gerardo, C*omercio electrónico: conceptos y reflexiones básicas*, Buenos Aires, Instituto para la Integración de América Latina y el Caribe, INTAL, 1999, p. 10.
[204] Almansa Martínez, Ana y Castillo Esparcia, Antonio, *op. cit.*
[205] León García, Omar, "Aplicación de las tecnologías de información y comunicación, en los procesos de innovación empresarial" *Revista de investigaciones*, vol. 11, núm. 1, junio 2018.

responsabilice de que el servicio que ofrece alerte y proteja a los usuarios frente a invasiones indebidas e ilegales a su vida privada[206]".

Al percatarnos de la importancia que ha tomado la protección de la información, es necesario aclarar qué, las definiciones de su protección han tomado su forma a través de las necesidades que han experimentado por el avance tecnológico.

La seguridad de la información y la seguridad informática, son dos cosas que no deben de confundirse, toda vez que cada es una determinante directa de la clasificación de información y depende directamente de los recursos y las formas que sean utilizadas para llevarlas a cabo.

Valencia Duque y Orozco Álzate definen una y otra y hacen las debidas distinciones de la siguiente manera:

> …es necesario aclarar la diferencia entre seguridad informática y seguridad de la información, la cual radica en el tipo de recursos sobre los que actúa cada una. Mientras que la primera se enfoca en la tecnología propiamente dicha, i.e. en las infraestructuras tecnológicas que sirven para la gestión de la información en una organización, la segunda está relacionada con la información en sí misma, como activo estratégico de la organización[207]

De acuerdo con lo aseverado en párrafos precedentes, los autores coinciden en determinar que la seguridad informática se refiere a todos los elementos técnicos y de infraestructura que permiten una adecuada protección de información, es decir, todos los sistemas de infraestructura diseñados para tener a salvo la información, por otro lado, las seguridad de la información puede considerarse a toda aquella cuya principal finalidad es definir el valor de la información, el contener una adecuada protección a la seguridad de la

[206] Peschard Mariscal, Jacqueline, "Protección de las niñas, niños y adolescentes en el ámbito digital: responsabilidad democrática de las instituciones de gobierno y de las agencias de protección de datos" en Gregorio, Carlos y Órnelas Lina (comp.), *Protección de datos personales en las redes sociales digitales: en particular de niños y adolescentes. Memorándum de Montevideo,* México, Instituto Federal de acceso a la información y protección de datos, julio 2011, p. 14.

[207] Valencia Duque, Francisco Javier y Orozco Álzate, Mauricio, "Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000" *Revista Ibérica de Sistemas e Tecnologias de Informação*, Manizales, Scielo Portugal, núm. 22, junio 2017, p. 75.

información, permitirá que el principal activo que es la información, cuente con políticas claras que garanticen una adecuada gestión y protección de información, dentro de los sectores que la administren, en este caso en específico, dentro del sector empresarial.

Se ha llegado a afirmar que de estos dos conceptos, con el que inició todo el concepto de protección, fue con el de derecho de la información, ya que se identificaba como la protección de cualquier tipo de información almacenada y tratada por cualquier medio, ya fuere físico o digital; ahora, con la aparición de las tecnologías de la información y de las comunicaciones el concepto se modificó para englobar a los elementos técnicos que permiten esa protección de información, toda vez, que no es necesario con definir la forma con la que debe de protegerse la información, también es necesario conocer que herramientas tecnológicas permitirán que eso sea posible.

Por otro lado, la integración de datos para los autores Martínez Valverde y Rojas Ruiz "se refiere al estado en el que se encuentran los datos, atendiendo a los posibles riesgos de corrupción"[208]. Hay que tener en claro la consideración de que al día de hoy una de las herramientas más costosas para cualquier empresa en el sistema de informático de seguridad que integren a su organización, toda vez, que el más remoto pensamiento de no contar con un sistema de seguridad adecuado resultará sin lugar a dudas, un problema económico, comercial y social, tal y como lo señala el autor Andrés Blasco "no sólo está en peligro la información estática almacenada en los discos de los sistemas protegidos por cortafuegos, etc. La información dinámica, la que viaja, puede ser vulnerable si no se toman las medidas necesarias (cifrado, firma electrónica, etc.)"[209]

También es importante tener perfectamente entendido lo señalado por Andrés Blasco "un sistema completamente seguro es aquél que se encuentra sin conexión a la red, apagado, desenchufado y metido dentro de una caja fuerte inexpugnable, cuya combinación solo conoce una persona el año pasado"[210]. El autor acierta en esta definición al señalar que una vez que algo se encuentre en la

[208] Martínez Valverde, José Fulgencio y Rojas Ruiz, Fernando, *op.cit.,* p. 22.
[209] Andrés Blasco, Javier de, *op. cit.,* p. 83.
[210] *Ibidem*, p. 72.

red, jamás podrá ser completamente seguro, siempre existirá el riesgo de que la información que nosotros proporcionemos, confiemos o almacenemos en algún sistema de información propio o de terceros, una vez conectados a la red, sea conocida, trasmitida y manipulada por algún tercero.

Como sabemos que en la actualidad es prácticamente imposible que se pueda llevar a cabo este tipo de candados contra el avance tecnológico, hay que reconocer que más allá de estar cuidando contra el mundo nuestra información, es necesario exigir a los proveedores productos y servicios que creen las medidas de seguridad adecuadas para que la información se proteja lo más claro posible, la seguridad desde el diseño es lo más importante en estos casos, toda vez que deberá de garantizarse que los datos recabados para un fin determinado no se sustraigan de manera ilegal por algún tercero y que éstos sean utilizados para fines que no fueron autorizados desde un principio.

Entre algunas de la propuestas de protección que a lo largo del tiempo se han venido desarrollando, se encuentran las de las autoras Navas Navarro y Camacho Clavijo, quienes afirman que "los sistemas de seguridad pueden ser de los más variados: sistemas de criptografía asimétrica, con doble clave (privada y pública), que mejoren o perfeccionen los ya existentes, claves de autenticación o de acceso, envío de SMS con claves determinadas, cambios constantes de claves, uso de la firma electrónica, sistemas de autenticación a través de *Facebook* o *Google,* etc."[211]. La seguridad transaccional es las primeras cosas que los usuarios del *e-commerce* exigen al momento de comprar en línea, esto debe de quedar establecido que no debe de depender del proveedor de servicios, si no de la plataforma que ayude a realizar este tipo transacciones, la cual debe de garantizar un nivel adecuado de protección de los datos y sobretodo de confidencialidad de la información.

Es importante señalar que este tipo de sistemas han sido completamente adaptados a algunos de los sistemas bancarios que operan en la actualidad, tal es el caso de BBVA Bancomer.

[211] Navas Navarro, Susana y Camacho Clavijo, Sandra, *op.cit.,* p.58.

BBVA Bancomer no solo se ha esforzado por estar en la vanguardia en la generación de tecnología apropiada que permita el adecuado tratamiento de protección de datos, también ha realizado esfuerzos significativos por hacer que la información tratada sea utilizada de acuerdo al marco de la LFPDPPP en México, para que puedan esos mismos datos, producir información que permita "obtener mejoras en sus productos, identificar necesidades y patrones de comportamiento"[212].

Para ellos su principal objetivo es llegar a esa información de valor involucrando a varias entidades a través de cantidades significativas de información, pero también cuidando en todo momento que la información sea protegida en cuanto a la confidencialidad, por lo que, se han considerado la utilización de algoritmos que permiten "establecer criterios matemáticos que aseguran que la información de las personas, comercios y entidades se mantengan de forma privada. El algoritmo de privacidad o competencia tiene como objetivo que no se proporcionen estadísticas agregadas en el caso de que esta información pueda poner en riesgo la ley de privacidad"[213]. Asimismo se ha comenzado a implementar la llamada condición acumulada, que permite que se puedan almacenar cantidades significativas de información, pero que una vez reunidas de manera conjunta, no sea posible que se pueda identificar de manera particular un dato considerado como privado[214].

Aunque se hace alusión del anterior ejemplo, con la conciencia de que se trata de una empresa dedicada al sector financiero, se toma como ejemplo debido a la calidad del software que permite que la información se encuentre lo más protegida posible, debido a su numeración aleatoria y encriptación de datos, solo por mencionar algunos ejemplos.

---

[212] Reyna, Armando, *Los algoritmos y la protección de datos*, México, BBVA, 2018, *https://www.bbva.com/es/podcast-coches-autonomos-la-revolucion-en-el-transporte-ya-esta-aqui/*

[213] *Idem.*

[214] *Idem.*

4.6.1. Auditoria web

La auditoria web por parte de las personas físicas y cualquier empresa que maneje un *e-commerce*, podría suponerse como una primer revisión obligatoria al cumplimiento del RGPD, toda vez que deberá de llevarse a cabo un análisis de riesgos o evaluaciones en materia de protección de datos, para saber hasta qué nivel de protección exige el reglamento en relación con el tipo de negocio que se tenga y los tipos de servicios que se ofrezcan.

Puede considerarse como una evaluación de impacto de protección de datos personales, a todos aquellos análisis, primeramente para saber el tipo de datos que serán recabados y las finalidades para los que serán empleados, y a partir de ahí poder medir el grado de responsabilidad y el número de obligaciones que deberán de adoptar para cumplir con la protección de información, una vez realizado lo anterior, la empresa podrá deducir el grado de responsabilidad que tiene y así adoptar las medidas necesarias para mitigar cualquier riesgo.

Es menester considerar que una evaluación de cumplimiento normativo que puede ofrecer una auditoria web ayudará considerablemente a la empresa a conocer el nivel de protección que efectivamente ofrece a los *ciberconsumidores*, y ayuda a conocer de primer momento si se cumple con una normativa, o en hasta qué punto cumple con alguna disposición legal de tratamiento de datos.

Asimismo, cuenta con beneficios como los de previsión, toda vez que, si derivado de una evaluación se logran identificar operaciones de tratamiento considerados como riesgosos, o se llega a identificar datos que son considerados como sensibles, se podrán adoptar las medidas adecuadas para cumplir con los estándares de protección.

Es importante recalcar que el propio RGPD, establece la obligación de los responsables de evaluar el impacto del tratamiento, previo al mismo tratamiento; lo anterior, con la finalidad de conocer la gravedad que pudiera resultar del tratamiento de información, así como informar las medidas que deberán de tomarse para mitigar cualquier riesgo.

Una evaluación de impacto es obligatoria de acuerdo con el Reglamento, siempre y cuando se identifiquen que las finalidades del tratamiento son

consideradas de alto riesgo, y que en tal situación, el responsable considerará que no cuenta con las medidas adecuadas para la protección.

De acuerdo con lo señalado en el artículo 35 del RGPD, el responsable deberá realizar la evaluación de impacto de los procesos de tratamiento de datos personales siempre que se dé alguna de las siguientes situaciones.

1. Cuando sea probable que un tipo de tratamiento, en particular si utilizan tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas.

a) Cuando se lleve a cabo la evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar.
b) Cuando se realicen tratamientos de datos a gran escala de las categorías especiales de datos o de los datos personales relativos a condenas e infracciones penales.
c) Cuando se realice la observación sistemática a gran escala de una zona de acceso público.

Para que una empresa conozca qué tipo de obligaciones son las que se estará sujetando a cumplir, primeramente deberá conocer las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y esto podrá cumplirse de manera directa y sin prejuicios, si se somete a una auditaría web, solo así estará en posibilidades de conocer de manera real las necesidades que tiene su *e-commerce* y a cumplir la conformidad con el RGPD, conociendo de primera mano los derechos e intereses legítimos de los titulares de la información.

4.6.2. Seguridad del sitio desde el diseño y por defecto

Partiendo de lo estipulado por el RGPD, existen dos principios para el cumplimiento efectivo de la normativa y para la implementación efectiva de la responsabilidad proactiva, el primero de ellos es la protección de datos desde el diseño y el segundo la protección de datos por defecto.

Se considera al principio de protección de datos desde el diseño como la protección de datos que debe de estar presente desde las primeras fases de concepción de un proyecto y formar parte de la lista de elementos a considerar antes de iniciar las sucesivas etapas de desarrollo. Estos requisitos se van a traducir en medidas técnicas y organizativas con el objeto de aplicar de forma efectiva los principios de protección de datos e integrar las garantías necesarias en el tratamiento[215]. En este caso debe de considerarse que si una empresa que conoce desde un inicio que va a tratar datos a través del comercio electrónico, debe de contemplar la protección de la información que recogerá y tratará para implementarla en el diseño de sus página web o aplicación móvil.

El término de la protección de datos por diseño, aunque hasta ahora es contemplado en una legislación, y sobre todo en una legislación de carácter internacional, no quiere decir que es un concepto completamente nuevo, tampoco los fines que pretender alcanzar "El concepto del *Privacy by Design* ha sido desarrollado por *el Informationand Privacy Commissioner of Ontario* de Canadá desde los años1990 y aparece por la primera vez en un informe que realiza esta autoridad de control con la autoridad de control holandesa publicado en 1995"[216].

En sus inicios, el concepto fue utilizado para sentar las bases sobre un tema que la tecnología comenzaba a cuestionarse, acerca de qué tan seguro es la privacidad a través de sistemas de intercambio de información interconectada entre sí, por lo que se propuso crear una filosofía que permitiera contemplar la posibilidad de crear un sistema que protegiera desde su creación, la información que tuviera a su alcance, sin importar su uso, medios de almacenamiento o finalidad para la que fuera empleada.

Posteriormente, en el año de 2012, la *Federal Trade Commission* puso al concepto de *Privacy by Design,* como un pilar dentro de los reglamentos de privacidad, toda vez que se consideraba desde entonces que las compañías

[215] Ortiz Amaya, Jesús, *Creación de una guía de apoyo para responsables y encargados de tratamiento basados en el Reglamento General de Protección de Datos Europeo*, trabajo de fin de grado en Ingeniería informática, Valencia, Universidad Politécnica de Valencia, p.26-35.

[216] Duaso Cales, Rosario, "Los principios de protección de datos desde el diseño y protección de datos por defecto", *en* Piñar Mañas, José (Dir.), *Reglamento general de protección de datos*, Madrid, Reus, 2017, p. 298.

debían de garantizar en todo momento la privacidad de los datos personales de los consumidores[217].

Lo anterior sirvió de base para que en el 2012 el grupo de trabajo encargado de la elaboración del RGPD incluyera los principios de la protección de datos desde el diseño y por defecto, como un lineamiento positivo para cumplir con la protección de información, toda vez que se consideró que al estar regulado dentro del reglamento, permitiría su conocimiento directo del tema, simplificando y aportando coherencia a la forma en que deben de protegerse los datos personales, tal y como lo señala Duaso Cales:

> En el contexto actual, dominado por unas tecnologías que permiten una interconexión permanente y una circulación sin límites de la información de carácter personal, integrar la privacidad en la arquitectura de todo sistema o aplicación así como en el diseño de aquellos procesos que conllevan el tratamiento de datos constituye una respuesta que puede traer resultados que ayuden al cumplimiento de los principios de protección de datos que las leyes establecen[218]

Por su parte, al momento de hablar de la protección de datos por defecto, puede definirse que se trata de delimitar el tratamiento de los datos personales, únicamente para cumplir con su objeto y finalidad, para que éstos sean estrictamente necesarios, inclusive si no fuera necesario el tratamiento de datos, y para que se abstengan de propio tratamiento.

En el caso del comercio electrónico, el considerar que no se traten datos personales no es posible, para que pueda perfeccionarse la compra-venta de bienes o servicios es necesario que se intercambie información para la perfección del contrato, y el realizarlo a través de medios electrónicos, se considera de primera necesidad que se intercambien datos para que la finalidad pueda llevarse a cabo. Por lo anterior, hay que considerar en todo momento al *e-commerce* con la funcionalidad del diseño por defecto para limitar el tratamiento de datos, no así para negar la recolección y tratamiento de los mismos.

---

[217] *Ibidem*, p. 299.
[218] *Idem.*

Para que pueda llevarse a cabo el principio de protección de datos por defecto, deberá de considerar el responsable, al menos los siguientes puntos relevantes:

a) Considerar la recolección de datos desde un criterio de minimización.
b) Debe analizar los procesos asociados a dichos tratamientos para que se acceda a los mínimos datos personales necesarios para ejecutarlos.
c) Debe implementar una política de conservación de datos que permita, con un criterio restrictivo, eliminar aquellos datos que no sean estrictamente necesarios.
d) Debe limitar el acceso por parte de terceros a dichos datos personales[219].

Es menester recalcar que si se implementa en las empresas esta herramienta, se estaría dando cumplimiento a uno de los artículos más importantes del RGPD, en este caso su artículo 25 establece directamente la protección de datos desde el diseño y por defecto. En dicho artículo la propia UE reconoce que considerando el estado de la técnica, el coste de la aplicación, la naturaleza de la información y su contexto y fines del tratamiento, deberán de implementarse en todo momento posible medidas técnicas y organizativas apropiadas que permitan cumplir con los derechos de los interesados.
De acuerdo con lo señalado en el artículo 25.2, deberá de garantizar que “por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas".

Las plataformas electrónicas dedicadas al *e-commerce* deberán configurarse desde el diseño de su programación con sistemas de intercambio electrónico de datos, en entornos cerrados de comunicación, por señalar un ejemplo; y deberá ponerse especial énfasis en los sistemas de identificación sólo con los datos pertinentes, y necesarios para llevar a cabo la transacción electrónica, según el papel de cada sujeto que intervenga. El diseño y gestión de

[219] *Ibidem,* p.298.

la plataforma habrá de tener en cuenta las específicas normas relativas al acceso a la información de las partes al procedimiento de mediación.

Asimismo, el cumplimiento por parte de empresas que estén constituidas por terceros países fuera de la UE, es imprescindible para que se encuentren en cabal cumplimiento de la normativa del RGPD. El considerando número 108 de dicho reglamento, señala que “en ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado”. En dichas situaciones, el propio reglamento propone a los terceros países incorporar normas corporativas vinculantes entre los países, clausulas tipo de protección de datos que se encuentren adecuadas a los lineamientos que exige el reglamento, así como cláusulas contractuales que previamente autorice una autoridad de control vinculada. El propio considerando señala como casos concretos la protección de información a través de los principios generales que lo regulan y de la protección de datos desde el diseño y por defecto.

Es menester señalar que, dentro de los objetivos de este principio está el contemplar en esta era tecnológica, un enfoque que signifique una pro actividad dentro del tratamiento de datos personales; es decir, no es intención del legislador el señalar una serie de requisitos y limitantes que obstaculicen el libre ejercicio de los responsables y encargados de la protección de datos, sino que se les proporcionen una serie de lineamientos que permitan tener una posición controlada, incentivando en todo momento el principio de precaución y pro actividad con el que deben de contar las empresas.

De igual forma, para que pueda considerarse cabalmente la protección de información a través de estos principios, se han recomendado la aplicación de siete principios fundamentales, los cuales me permito transcribir a continuación:

1. Proactivo, no reactivo; Preventivo no correctivo.
2. Privacidad como la configuración predeterminada.
3. Privacidad incrustada en el diseño.
4. Funcionalidad total – «Todos ganan», no «Si alguien gana, otro pierde».
5. Seguridad Extremo-a-Extremo – Protección de ciclo de vida completo.
6. Visibilidad y Transparencia-Mantenerlo abierto.

7. Respeto por la Privacidad de los usuarios-Mantener un enfoque centrado en el usuario[220]

El poder implementar todos estos principios desde la creación de un sitio web o aplicación móvil que tenga como finalidad el comercio electrónico transnacional, traería consigo diversas ventajas que beneficiarían principalmente a las MiPyMEs, toda vez que, ellas por su escasa capacidad organizativa, económica y de conocimiento legal, les sería de gran ayuda insertar desde el inicio de sus sitios, la protección tecnológica necesaria para que de manera automática proteja los datos personales que traten directa o indirectamente, se considera que es una opción adecuada que permitirá ahorrar costes y tiempos de ejecución, imprescindibles para aquellos que comienzan un comercio electrónico transnacional.

4.6.3. Corresponsables del tratamiento

Una de las herramientas que puede pueden utilizar las empresas para cumplir debidamente con lo que establece elRGPD, es la contratación de servicios que ayuden a proteger y tratar de una forma correcta la información.

Esta herramienta será de gran utilidad para las grandes empresas quienes además de tratar desde el diseño y por defecto la información, se apoyarán de manera constante a través de expertos en protección de información, en los requerimientos legales que establece la UE.

El responsable de la información, quienes son en este caso las empresas dedicadas al *e-commerce*, deberán de elegir un encargado que ofrezca garantías adecuadas y suficientes para implementar y mantener en todo momento, las medidas técnicas y legales que el propio RGPD establece, y así garantizar la protección de los derechos de los titulares de la información.

Para que lo anterior quede perfectamente establecido y delimitado en cuanto obligaciones entre el responsable y el encargado, deberá de existir

[220] Cavoukian, Ann, *Privacy by Design, The 7 Foundational Principles*, Ontario, 2009, *https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf*

previamente un contrato de prestación de servicios que los vincule, en donde se establezca de manera puntual cada una de las obligaciones que se les va a transferir al encargado de la información, de igual forma el contrato deberá de contener los requisitos mínimos que señale el RGPD, para los comercios electrónicos, así como los derechos a los que el titular de la información tendrá derecho durante toda la relación contractual. “Si por el contrario es un acto jurídico, puede basarse en clausulas tipo por la comisión europea o por la autoridad de control competente”[221].

Para las grandes empresas será de mucha utilidad el que puedan estar más seguros en cumplimiento de obligaciones, de privacidad y protección y sobretodo de cumplimiento de un reglamento de carácter internacional. Será un alivio para las empresas responsables de la información si transfieren esa obligación, apoyándose mediante prestadores de servicios especializados en protección de información, medios electrónicos y que tengan un amplio conocimiento técnico y legal en la materia.

Es menester recalcar que no debe considerarse como una liberación de responsabilidad del responsable directo de la información, toda vez que sin perjuicio de la contratación de un encargado de la protección de la información, el deber de confidencialidad y protección de datos, siempre será compartida, tanto el responsable como el encargado tendrán una proporción compartida de obligaciones.

Por motivo de lo anterior, será de vital importancia que el responsable del tratamiento de datos, sea en todo momento diligente a la hora de elegir a un encargado de tratamiento, comprobando previamente que éste, reúna garantías técnicas suficientes, asegurándose en todo momento de que de que se cumplan adecuadamente sus instrucciones. El encargado de la información debe de cumplir con las obligaciones que el responsable le encomiende, así como seguir las instrucciones específicas para el tratamiento de datos y abstenerse de destinarlas para otras finalidades.

[221]Cotino Hueso, Lorenzo, “Confidencialidad y protección de datos en la mediación en la Unión Europea, *Revista del Instituto de Ciencias Jurídicas de Puebla*, Puebla, nueva época, vol. 12, núm. 41, ene-jun 2018, p. 329.

Otra de las cosas que deberán de garantizar los encargados de la información, es que cumple con los estándares de protección que solicita la UE.

De igual forma, existe la posibilidad de que puedan contratarse los servicios de encargados que actúen en un país tercero, tal es el caso de grandes empresas dedicadas al alojamiento web o servicios de la nube, operadores de información o telecomunicaciones; por lo que, en tales situaciones, el encargado de la información deberá de asegurarse que esa transferencia de información sea adecuada y segura en el país en dónde será encargada, con los mismos niveles de protección que México pudiera ofrecérsele. “La Comisión Europea, hasta la fecha, ha adoptado once decisiones respecto Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay y Nueva Zelanda”[222].

Los países mencionados son -para la UE- países con estándares apropiados de información y en lo que se podría confiar para transferir de manera segura la información, sin embargo más allá del cumplimiento y seguridad que pudieran ofrecernos empresas de protección de información perteneciente a algunos de esos países. Es obligación de que las empresas que contraten sus servicios, estén en constante inspección de que se cumple con los estándares de protección que exige el RGPD y de las propias obligaciones que se le encomiendas a través de los contratos de prestación de servicios y de sus propias reglas corporativas.

[222] *Idem.*

CONCLUSIONES

La presente investigación ha permitido recopilar una serie de elementos básicos que acceden a comprender los principales ordenamientos que enuncia el RGPD de la UE. Su conocimiento y posterior análisis, ha dado como resultado la obtención de una perspectiva que permite crear una opinión aislada de la importancia de una renovación a la anterior directiva en materia de protección de datos personales que regía a la UE, los avances tecnológicos y las nuevas formas de comunicación, han provocado que se reformen los principios e ideas que se tenían sobre las directrices que protegen a nuestra nueva era considerada como "la era digital".

El conocer de primera mano las obligaciones que se desprender del RGPD es considerado, de acuerdo al presente trabajo, como una herramienta de importante valor, no solo por el conocer el avance legislativo que tiene la UE en temas de protección de información en el comercio electrónico, sino también para comprender las necesidades que dieron lugar a la creación de nueva normativa y a la actualización de temas que con el paso de los años y por la prácticas que se han venido creando, se consideran ahora como desfasadas o fuera de lugar, por lo que fue necesario crear nuevas medidas que otorguen una protección adecuada a las exigencias de la sociedad actual, a criterio propio, uno de los más importantes para toda persona es su privacidad.

De lo anterior, puede concluirse que el objetivo de la presente investigación se ha cumplido de manera satisfactoria, toda vez que se analizaron las principales obligaciones que el RGPD de la UE impone a las empresas dedicadas al *e-commerce* transnacional, entre ellas las empresas mexicanas.

Durante la presente investigación se cumplen con cada uno de los objetivos específicos señalados para la comprobación de la hipótesis planteada, toda vez que, en efecto, es necesario que las empresas mexicanas dedicadas al *e-commerce* transnacional hacia la UE implementen estándares de seguridad que protejan los datos personales dentro de sus plataformas electrónicas, la implementación del principio de diseño por defecto es considerada como la más práctica y económica para que cualquier empresa, sin importar su capacidad económica o recursos, pueda cumplir con la normativa y con obligaciones que derivan de ella.

Así mismo, se enuncian algunas de las conclusiones a las que se llegó través de la presente investigación:

PRIMERO. Del estudio de la protección de datos personales como un derecho fundamental se deduce que, el derecho a la privacidad, al derivar directamente del derecho a la intimidad y la autodeterminación informativa, es un derecho indispensable para ejercer de manera consciente y responsable. El contar con estándares de control que permitan vigilar y sobre todo decidir libremente a qué actores y para qué fines se proporcionan los datos es un avance significativo, que no solo proporciona beneficios económicos, también contribuye a que nuestra información se encuentre en buenas manos y que no se destinen los datos personales para contribuir al enriquecimiento de terceras personas que lucren con esa información.

El conocer la evolución histórica de la protección de datos personales permitió la compresión de los hechos que dieron lugar a la preocupación de los países del mundo para tomar la decisión de controlar la información, primero por cuestiones sociales y políticas y posteriormente por el valor económico que la información representa para medir el poder de una sociedad determinada.

De igual forma, el estudio de los organismos gubernamentales y privados que se encuentran en constante preocupación por los problemas actuales que derivan del flujo de información, nos hacen reflexionar sobre la importancia que representan los datos personales a nivel internacional. La UE ha hecho un trabajo excepcional al contemplar los cambios tecnológicos y sociales que se han

experimentado en los últimos años y, al elaborar nueva legislación, ha puesto a pensar a terceros países sobre la importancia de contar con estándares de seguridad que protejan la información de sus nacionales.

Por último, el capítulo primero refleja el trabajo conjunto y a su vez aislado que han desarrollado los países del mundo para proteger la información de carácter personal, es menester mencionar que México no dista de estar a la altura de las primeras potencias del mundo, al momento de referirse a la protección de datos personales; sin embargo, ha podido deducirse que la forma en la que México transmite la importancia de la protección de datos personales a sus ciudadanos no es suficiente, la legislación mexicana debe de ser más clara y atractiva para que pueda llamar la atención para el ejercicio del derecho a la privacidad y sobre todo para que se ejerza de manera adecuada.

SEGUNDO. Del estudio de la protección de datos dentro del comercio electrónico se llega a deducir en primer término, la importancia del reconocimiento de la figura del *e-commerce* en nuestra actualidad. La consolidación de nuevas formas de comercio basados en las TICs es producto de la evolución natural de la sociedad utilizando nuevos métodos tecnológicos. Asimismo se reconoce que la actividad del comercio no tiene un cambio sustancial como tal, es decir, no se rompe con la esencia que el comercio ha tenido durante épocas milenarias, el intercambio de productos y servicios por medio de un precio determinado continúa intacto. Los principios básicos de neutralidad tecnológica, equivalencia funcional y no alteración del derecho pre-existente, son gran prueba de ello.

Con respecto a la protección de información dentro del *e-commerce*, es menester mencionar que a nivel internacional se cuenta con un avance significativo en la materia, el RGPD es prueba clara de ello dirigiendo su legislación principalmente al comercio electrónico; por otro lado, es importante reconocer que el comercio electrónico está en constante cambio, por lo que, no debe afirmarse que los lineamientos ahora planteados por las legislaciones internacionales son justo lo que el comercio actual necesita. Sin embargo, se ha transmitido la necesidad de proteger la información dentro del *e-commerce*, el mal

uso de la información obtenida a través de dichas prácticas mercantiles, puede provocar pérdidas incalculables, tanto pecuniarias, como sociales.

TERCERA. Al llevar a cabo el estudio de las principales disposiciones legales que emanan del RGPD, se llegó a la conclusión de que el reglamento es un ordenamiento legal innovador y arriesgado que apuesta por la creación de un mercado único digital, para la UE, la protección de la información es pieza clave para el cumplimiento de sus objetivos, entre ellos, una comunicación segura con los países que integran la UE, así como con los demás países del mundo. La UE al visualizar el excesivo flujo transfronterizo de datos personales fuera de su esfera de aplicación de la UE, ha dado lugar a tomar la decisión de extender la responsabilidad a terceros países; es justificable su punto de vista, la información hoy en día puede considerase como el nuevo petróleo y es claro que la UE no se encuentra en disposición de permitir que se haga un uso indebido de ellos, por lo que es estricta con los lineamientos que ha establecido a cualquier tercer país que tenga contacto con información de carácter personal de sus nacionales.

De igual forma se concluye que, el RGPD no es un ordenamiento que nació de cero, normativas antecesoras como la directiva 95/46/CE y el convenio 108 del consejo de Europa fueron importantes ordenamientos que sentaron bases a las necesidades de la UE para proteger adecuadamente la protección de carácter personal.

Los principios insertados en el RGPD demuestran la necesidad de garantizar a la brevedad lo dispuesto en el reglamento, el establecer lineamientos que garantizan el derecho de acceso a la información, portabilidad de datos, control de información y el derecho a la supresión de datos, han provocado que terceros países, como es el caso de México, contemplen de manera interna la necesidad de regular esos derechos a su propia legislación.

El RGPD es una herramienta primordial para proteger el comercio electrónico internacional, sin embargo al ser tan reciente y sobre todo tan exigente en cuestiones de tecnología, dista de ser una legislación de aplicación absoluta, ya ha comenzado a cuestionarse sobre su aplicación, no por el hecho de ser de reciente aplicación, sino por las dificultades a las que las empresas se están

enfrentando para implementar las disposiciones legales a sus *e-commerce*, la falta de capacitación, comprensión legal y sobretodo solvencia económica, dejan de lado, la eficaz aplicación del reglamento.

CUARTO. Hablando del comercio electrónico nacional y tomando como punto de referencia a México como un país tercero para la UE, los capítulos precedentes de la presente investigación fueron imprescindibles para comprender la importancia que tiene el comercio electrónico hoy en día. México ha comenzado con presencia internacional gracias a las TICs, sin embargo, debe de acatar a las nuevas reglas que impone el comercio impuesto por la UE, si es que desea mantener relaciones comerciales en buenos términos.

El comercio electrónico transnacional mexicano hacia la UE está surgiendo a paso lento; sin embargo, la que suscribe augura que con la celebración de los tratados con los que actualmente cuentan ambas naciones, se abra paso a nuevas formas comerciales.

A través de la presente investigación se identificaron los principales retos que tienen las empresas mexicanas dedicadas al *e-commerce* transnacional en la UE y se concluyeron otros. Por un lado, en México existen varios retos dentro del comercio electrónico nacional y transnacional, que primero deben ser de tratados de manera interna, uno de esos retos es generar la confianza hacia el consumidor de que sus datos personales están resguardados de manera segura. Se considera que si México logra trasmitir y sobretodo demostrar que cuenta con adecuados estándares de seguridad de los sitios que utiliza para llevar a cabo su *e-commerce* transnacional, podrá ganar la confianza de sus clientes nacionales y extranjeros.

Esta investigación ha llegado a deducir que es necesario que México cumpla con los lineamientos que el propio RGPD estipula, lo cual será suficiente para consumar su objetivo principal, cumplir con una legislación de carácter internacional que le permitirá crear relaciones comerciales con los ciudadanos de la UE y, por otro lado, creará un ambiente de confianza para que tanto los consumidores nacionales como extranjeros puedan apoyar al comercio nacional y que éste comience a despegar.

FUENTES DE INFORMACIÓN

Bibliografía

ABAD ALCALÁ, Leopoldo, “La lucha por la intimidad en Internet”, *La libertad de información*, Madrid, Seminario Complutense de telecomunicaciones e información, 2001, pp. 198-205, *http://pendientedemigracion.ucm.es/info/cyberlaw/actual/9/leg04-09-01.htm*

ALVARADO BENÍTEZ, Laura Margarita y ROBLES ESTRADA, Celestino, “La percepción acerca de la privacidad y seguridad en el social *e-commerce* en México: Un estudio exploratorio”, *La mercadotecnia digital y en redes sociales*, Guadalajara, Red Internacional de Investigadores en Competitividad, 2012, pp. 634-646.

ANTEMPORLATINAM VALERO, José María, “Definición de comercio electrónico”, *Relevancia del ecommerce para la empresa actual*, Valladolid, tesis para obtener el grado de doctor, 2014.

ANDRÉS BLASCO, Javier de, “¿Qué es el Internet?”, en GARCÍA MEXIA, Pablo (director), *Principios de derecho de* Internet, 2a ed., Valencia, Tirant lo Blanch, 2005, pp. 76-91.

ARELLANO, Paloma*, El Comercio Electrónico,* México, UNAM, *https://archivos.juridicas.unam.mx/www/bjv/libros/7/3259/6.pdf.*

CARO GONZÁLEZ, Arianis Suzeti, et al, *Plan estratégico de la Empresa Uber 2019-2023*, Lima, Trabajo de Investigación presentado para optar al Grado Académico de Magíster en Administración, 2019.

CASTELLS, Manuel, *Internet y la sociedad red,* Barcelona*,* La Factoría, vol. 14, 2001.

CAVOUKIAN, Ann, *Privacy by Design, The 7 Foundational Principles*, Ontario, 2009, *https://www.ipc.on.ca/wpcontent/uploads/resources/7foundationalprinciples.pdf*

CENTRO DE ESTUDIOS INTERNACIONALES GILBERTO BOSQUES, "Principales aspectos del nuevo Tratado de Libre Comercio entre México y la Unión Europea (TLCUEM): oportunidades, logros y desafíos", Nota de Coyuntura, México, Senado de la República, 3 de mayo de 2018.

COLMENAREJO FERNÁNDEZ, Rosa, *Una ética para Big data: introducción a la gestión ética de datos masivos*, Barcelona, UOC, 2018.

DUASO CALES, Rosario, “Los principios de protección de datos desde el diseño y protección de datos por defecto”, *en* PIÑAR MAÑAS, José (Dir.), *Reglamento general de protección de datos*, Madrid, Reus, 2017, pp. 295-320.

GARCÍA MEXÍA, Pablo, “*La singular naturaleza jurídica del reglamento general de protección de datos de la UE, sus efectos en el acervo nacional sobre protección de Datos”, en* PIÑAR MAÑAS, José (Dir.), *Reglamento general de protección de datos*, Madrid, Reus, 2017, pp. 23-34.

GARRIGA DOMÍNGUEZ, Ana, *Tratamiento de datos personales y Derechos Fundamentales*, Madrid, Dykinson, 2014.

GARRIGA DOMÍNGUEZ, Ana, *Tratamiento de datos personales y Derechos fundamentales: Desde Hollerith hasta Internet*, México, HuriEge, consolider ingenio, 2010.

GARIBOLDI, Gerardo, C*omercio electrónico: conceptos y reflexiones básicas*, Buenos Aires, Instituto para la Integración de América Latina y el Caribe, INTAL, 1999.

GAYTÁN TORRES, Ricardo, *Teoría del comercio internacional*, 25ª ed., México, Siglo XXI, 2005.

KATARZYNA GOLINSKA, Mónica*, La evolución normativa del Derecho a la Protección de Datos*, Alcalá de Henares, Universidad de Alcalá, 2018.

LÓPEZ SÁNCHEZ, Manuel Ángel, *Derecho mercantil I*, Pamplona, 2009.

LUCAS MURILLO DE LA CUEVA, Pablo, *El derecho a la autodeterminación informativa*, Madrid, Tecnos, 1990.

LUJAN MORA, Sergio, *Programación de aplicaciones web: historia, principios básicos y clientes web, Alicante*, Club Universitario, 2002.

MALDONADO OTERO, Claudia, *Ley Federal de Protección de Datos Personales en Posesión de los Particulares en México*, México, UNAM, 2017.

MARTÍNEZ VALVERDE, José Fulgencio y ROJAS RUIZ, Fernando, *Comercio electrónico*, Madrid, Paraninfo, 2016.

NAVA GONZÁLEZ, Wendolyne y BRECEDA PÉREZ, Jorge Antonio, *México en el contexto internacional de solución de controversias en línea de comercio electrónico,* México, UNAM, 2017.

NAVAS NAVARRO, Susana y CAMACHO CLAVIJO, Sandra, *Mercado digital, principios y reglas jurídica*s, Valencia, Tirant lo Blanch, 2016.

ORGANIZACIÓN MUNDIAL DEL COMERCIO, Comercio electrónico, 2017, *https://www.wto.org/spanish/tratop_s/ecom_s/ecom_s.htm.*

OROPEZA, Doris, *La competencia económica en el comercio electrónico mexicano y su protección en el sistema jurídico mexicano*, México, UNAM, Instituto de investigaciones jurídicas, 2018.

ORTÍZ AMAYA, Jesús, *Creación de una guía de apoyo para responsables y encargados de tratamiento basados en el Reglamento General de*

Protección de Datos Europeo, trabajo de fin de grado en Ingeniería Informática, Valencia, Universidad Politécnica de Valencia.

PABLOS HEREDERO, Carmen de *et al*, *Organización y transformación de los sistemas de información de la Empresa*, 4a ed., Madrid, ESIC, 2019.

PESCHARD MARISCAL, Jacqueline, "Protección de las niñas, niños y adolescentes en el ámbito digital: responsabilidad democrática de las instituciones de gobierno y de las agencias de protección de datos" en GREGORIO, Carlos y ORNELAS Lina (comp.), *Protección de datos personales en las redes sociales digitales: en particular de niños y adolescentes. Memorándum de Montevideo,* México, 2011, pp. 21-26.

PENDÓN MELÉNDEZ, Miguel Ángel, *La perfección del contrato en Derecho Privado*, Valencia, Tirant lo Blanch, 2009.

PILLOU, Jean-François, *Introducción al comercio electrónico (e-Commerce)*, junio 2017, *http://es.ccm.net/contents/201-introduccion-al-comercio-electronico-e-commerce.*

POLANCO LÓPEZ, Hugo Armando, *Manifestaciones del principio de equivalencia funcional y no discriminación en el ordenamiento jurídico Colombiano*, Santiago de Cali, Criterio Jurídico, 2017.

REBOLLEDO DELGADO, Lucrecio, *Vida privada y protección de datos: Un acercamiento a la regulación internacional Europea y Española*, México, UNAM.

RECIO GAYO, Miguel, *Protección de Datos Personales e Innovación ¿(in)compatibles?,* Colección de Derechos de la Nuevas Tecnologías, Madrid, Reus, 2016.

REYNA, Armando, *Los algoritmos y la protección de datos*, México, BBVA, 2018, *https://www.bbva.com/es/podcast-coches-autonomos-la-revolucion-en-el-transporte-ya-esta-aqui/*

RIPOL CARULLA, Santiago, "Aplicación territorial del Reglamento" *en* PIÑAR MAÑAS, José (Dir.), *Reglamento general de protección de datos*, Reus, Madrid, 2017, pp. 77-95.

SALTOR, Carlos Eduardo, "Sobre el concepto del derecho a la intimidad", *La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación Argentina*, tesis doctoral para obtención de grado, Madrid, Universidad complutense de Madrid, 2013, pp. 185-187.

SOMALO PECIÑA, Ignacio, *El comercio electrónico: una guía completa para gestionar online*, Madrid, ESIC, 2017.

VALDÉS HERNÁNDEZ, Miguel Ángel, "Diagnóstico del comercio electrónico con base en la confianza, seguridad y conocimiento del consumidor final", *Red internacional de investigadores en competitividad,* México, vol. 8, núm. 1, 2014, p. 677, *https://www.riico.net/index.php/riico/article/view/1177/845.*

VERA SANTOS, José Manuel, “Derechos fundamentales, Internet y nuevas tecnologías de la información y de la comunicación”, en GARCÍA MEXIA, Pablo (director), *Principios de derecho de Internet,* 2a ed., Valencia, Tirant lo Blanch, 2005, pp. 211-246.

VIDAL, Gregorio, *Expansión de las empresas transnacionales y profundización del subdesarrollo: ¿Cómo construir una alternativa al desarrollo?*, México, Mimeo, UAM, 2005.

ZEBALLOS, Emilia, *La protección de datos personales en España,* Madrid, tesis para obtener el grado de doctora, Universidad Complutense de Madrid, 2013.

Hemerografía

ALMANSA MARTÍNEZ, Ana y CASTILLO ESPARCIA, Antonio, “Comunicación Institucional en España. Estudio del uso que los diputados españoles hacen de las TIC en sus relaciones con la ciudadanía”, *Revista Latinoamericana de Comunicación*, Quito, 2014, núm. 126, pp. 23-30

ASTUDILLO, Catalina *et al*, “Acometer contra un ERP con Software Libre”, *Enfoque UTE*, vol. 9, núm.1, Mar. 2018, pp. 138-148, *http://ingenieria.ute.edu.ec/enfoqueute/.*

BAEZ, Javier, “El comercio electrónico en México en 10 pasos”, *Dinero en Imagen*, *http://www.dineroenimagen.com/2015-04-14/53963.*

CAMACHO RODRÍGUEZ, Karla Teresa, “Reflexiones sobre la importancia de la noción de la clase social en los estudios de consumo. La relación de los jóvenes con las e-compras en México”, *Intersticios Sociales*, Guadalajara, año 9, núm. 17, marzo- agosto 2019, pp. 59-78.

CERDA SILVA, Alberto, “El nivel adecuado de protección, para las transferencias internacionales de datos personales desde la Unión Europea”, *Revista de Derecho Valparaíso*, núm. 36, pp. 327-356.

COTINO HUESO, Lorenzo, “Confidencialidad y protección de datos en la mediación en la Unión Europea”, *Revista del Instituto de Ciencias Jurídicas de Puebla*, Puebla, nueva época, vol. 12, núm. 41, ene-jun 2018, pp. 311-341.

“EL ESTADO DEL COMERCIO ELECTRÓNICO EN MÉXICO”, *El Economista*, 18 de noviembre de 2016, *https://www.eleconomista.com.mx/arteseideas/El-estado-del-comercio-electronico-en-Mexico-20161118-0169.html*

FUENSANTA MARTÍNEZ, MARTÍNEZ, Dolores, “Unificación de la protección de datos personales en la Unión Europea: desafíos e implicaciones”, *El profesional de la información*, Murcia, núm. 1, 2018, pp. 185-194.

GONZÁLEZ GRANDA, Piedad, “Protección judicial de consumidores y usuarios en el ámbito del comercio electrónico” *Revista para el Análisis del Derecho,* Barcelona, INDRET, núm. 4, *2007*, pp. 3-5.

GUARDIA, Carlos de la, “La evolución del comercio electrónico”, *Razón y palabra*, Estado de México, núm. 20, noviembre 2000, *http://www.razonypalabra.org.mx/anteriores/n20/20_cguardia.html.*

INSTITUTO FEDERAL DE ACCESO A LA INFORMACIÓN PÚBLICA, *La protección de datos personales en México: una propuesta para deliberar*, julio 2018, *http://iaipoaxaca.org.mx/biblioteca_virtual/datos_personales/5.pdf*

INSTITUTO NACIONAL DE ACCESO A LA INFORMACIÓN (INAI), C*ómo ejercer tu derecho a la protección de datos personales, http://inicio.ifai.org.mx/SitePages/Como-ejercer-tu-derecho-a-proteccion-de-datos.aspx?a=m1.*

LA COMISIÓN DE DERECHO CONSTITUCIONAL, LEGISLACIÓN Y ADMINISTRACIÓN GENERAL DE LA REPÚBLICA *Las implicaciones de las nuevas normas europeas para la Protección de datos personales en derecho Francés*. Informe de 4544, Asamblea Nacional, 22 de febrero de 2017.

MARTÍN, Javier, “Pixmania ocupa la calle”, *El País*, Barcelona, 20 de marzo de 2012, *http://tecnologia.elpais.com/tecnologia/2012/03/20/actualidad/1332232088_282597.html*

MARTÍNEZ MARTÍNEZ, Ricard, “El derecho fundamental a la protección de datos: perspectivas” *Revista de* Internet*, Derecho y Política*, septiembre 2007, pp. 48-71.

MARTÍNEZ MARTÍNEZ, Ricard, “Transformación digital y diseño orientado a la privacidad en la Universidad” *RUIDERAe: Revista de Unidades de Información*, Valencia, UCLM, núm. 13, 1er semestre 2018, p.2.

MENDOZA ENRÍQUEZ, Olivia, “Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento”*, Revista IUS*, Puebla, vol.12, núm.41, enero-junio 2018, pp. 268-291.

OJEDA BELLO, Zahira, “El derecho a la protección de datos personales desde un análisis histórico-doctrinal” *Tla-melaua*, Puebla, vol. 9, núm. 38, 2015, p. 58-71.

PRESAS MATA, Fátima, “La responsabilidad social de los skateholders en la publicidad: necesidad de un compromiso ético en la industria publicitaria”, *Methaodos. Revista de ciencias sociales*, Vigo, vol. 6, núm. 1, 2018, pp. 38-51.

PROAÑO, ESCALANTE, Rodrigo y GAVILANES MOLINA, Andrés, “Estrategia para responder a incidentes de inseguridad informática ambientado en la

legalidad ecuatoriana", *Enfoque UTE*, Marzo 2018, pp. 90-140, *http://ingenieria.ute.edu.ec/enfoqueute/*

TORNABENE, Inés, "Protección de Datos Personales: repasando un poco de Historia, del Tercer Reich a Facebook", *Revista CSO businessadvisor*, 26 de febrero de 2015, *http://www.cxo2cso.com/2015/02/proteccion-de-datos-personales.html.*

UNIVERSIDAD INTERNACIONAL DE VALENCIA *Acuerdos Comerciales Entre La Unión Europea Y Latinoamérica*, Valencia, Universidad Internacional de Valencia, 2015, p. 5-31, *https://eulacfoundation.org/es/system/files/informe-acuerdos-comerciales-entre-la-union-europea-y-latinoamerica.pdf*

VALENCIA DUQUE, Francisco Javier y OROZCO ALZATE, Mauricio, "Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000" *Revista Ibérica de Sistemas e Tecnologias de Informação*, Manizales, Scielo Portugal, núm. 22, junio 2017, pp. 73-88.

VÉLEZ MEDICI, Armando, "Nueva norma amenaza al 95% del e-commerce en México", *Theemag*, Ciudad de México, agosto 2018, *https://www.the-emag.com/blog/nueva-norma-amenaza-el-95-del-e-commerce-en m%C3%A9xico*.

VENEGAS, Eduardo, "Las cosas que los consumidores aman y odian de comprar online", *Revista Merca 2.0*, México, 22 de mayo 2017, *https://www.merca20.com/las-cosas-que-los-consumidores-aman-y-odian-de-comprar-online/.*

VELASCO SAN MARTÍN, Cristos, "Privacidad y protección de datos personales en Internet. ¿Es necesario contar con una regulación específica en México?", *Boletín de Política Informática,* México, núm. 1, 2003.

Derecho Positivo Internacional

COMISIÓN DE LAS NACIONES UNIDAS PARA EL DERECHO MERCANTIL INTERNACIONAL, Ley Modelo De La CNUDMI Sobre Comercio Electrónico (1996), consultado el 7 de noviembre de 2018, *http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/1996Model.html*

REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

PAQUETE DE NORMAS ISO/IEC 27000, Aspectos claves de su diseño e implantación, *www.isotool.org*

PROYECTO DE LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES (Antes denominado

proyecto de Ley Orgánica de Protección de Datos de Personales de Carácter Personal, Congreso de los Diputados, serie A, núm. 13-4, 17 de octubre 2018.

TRATADO DE LIBRE COMERCIO México- Unión Europea, Subsecretaría de Comercio Exterior, Secretaría de Economía, *http://www.bruselas.economia.gob.mx/swb/swb/bruselas/TLC_Mex_UE*

Derecho Positivo Mexicano

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, Última reforma DOF 29 de enero de 2016, México, Cámara de Diputados del H. Congreso de la Unión, *http://www.diputados.gob.mx/LeyesBiblio/pdf/1_270818.pdf*

CÓDIGO DE COMERCIO, Última reforma DOF 28-03-2018, México, Cámara de Diputados del H. Congreso de la Unión, *http://www.diputados.gob.mx/LeyesBiblio/ref/ccom.htm*

LEY DE LA PROPIEDAD INDUSTRIAL, última reforma DOF 18-05-2018, Cámara de Diputados del H. Congreso de la Unión, *http://www.diputados.gob.mx/LeyesBiblio/pdf/50_180518.pdf*

LEY FEDERAL DEL DERECHO DE AUTOR última reforma DOF 15-06-18, México, Cámara de Diputados del H. Congreso de la Unión, *http://www.diputados.gob.mx/LeyesBiblio/ref/lfda.htm*

LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR, última reforma DOF 09-04-2012, México, Cámara de Diputados del H. Congreso de la Unión, *https://www.profeco.gob.mx/juridico/pdf/l_lfpc_ultimo_CamDip.pdf*

LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTÍCULARES, última reforma DOF 05-07-2010, México, Cámara de Diputados del H. Congreso de la Unión, *http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf*

LEY FEDERAL DE TELECOMUNICACIONES Y RADIODIFUSIÓN, última reforma DOF 15-06-2018, México, Cámara de Diputados del H. Congreso de la Unión, *http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_020419.pdf*

PROYECTO DE NORMA MEXICANA PROY-NMX-COE-001-SCFI-2018, "Comercio electrónico-Disposiciones a las que se sujetarán aquellas personas que ofrezcan, comercialicen o vendan bienes, productos o servicios", Secretaría de Economía, México, Octubre 24, 2018.