***U**niversidad **M**ichoacana de **S**an **N**icolás de **H**idalgo*
***F**acultad de **D**erecho y **C**iencias **S**ociales*
***D**ivisión de **E**studios de **P**osgrado*

# LOS RETOS JURÍDICOS Y TÉCNICOS EN EL TRATAMIENTO DE DATOS PERSONALES EN LA NUBE POR LAS MIPYMES EN MÉXICO

**T E S I S**

Que para obtener el grado de

**Maestro en Derecho de la Información**

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

Flavio Suárez Muñoz

**DIRECTORA DE TESIS**

Dra. Rosa María de la Torre Torres

**CODIRECTOR**

Dr. Pedro Chávez Lugo

*Morelia, Michoacán, México* *Agosto/2020*

# AGRADECIMIENTOS

Agradezco al Consejo Nacional de Ciencia y Tecnología (CONACYT) por su patrocinio para realizar este proyecto de tesis, su apoyo fue de gran importancia en mi desarrollo profesional. Sin duda la inversión en la ciencia y la tecnología, son parte del esfuerzo que el Estado realiza para lograr un México mejor.

Agradezco a la Dra. Rosa María de la Torre Torres, directora de tesis, por su incondicional apoyo para hacer posible que este proyecto llegara a buen término.

De igual manera, agradezco al Dr. Pedro Chávez Lugo por su apoyo como codirector y revisor, su apoyo fue de gran valor en este trabajo.

Agradezco infinitamente al Dr. Juan Carlos Gonzáles Vidal por su dedicada labor en la revisión de este trabajo.

Extiendo un especial agradecimiento a mi esposa e hijos por el tiempo que me regalaron para poder terminar este proyecto.

A mi madre le agradezco la vida y el haberme enseñado a ser fuerte, a no caer y siempre caminar hacia adelante y comprender que nada es imposible cuando te lo propones. Gracias mamá.

# ÍNDICE

CAPÍTULO SEGUNDO

NATURALEZA JURÍDICA DEL DERECHO A LA INFORMACIÓN

CAPÍTULO TERCERO

RESULTADO DEL ANÁLISIS DE LOS AVISOS DE PRIVACIDAD

CAPÍTULO CUARTO

PROPUESTA JURÍDICO–TÉCNICA PARA LA ARMONIZACIÓN ENTRE TECNOLOGÍA Y EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

## ÍNDICE DE FIGURAS



## ÍNDICE DE TABLAS

*Si no vas hasta el final*
*¿por qué empezar?*
*- Joe Namath -*

## RESUMEN

La economía de México se encuentra sostenida mayormente por microempresas, las cuales, para poder hacer frente a las necesidades de la sociedad de la información, deben implementar el uso de las tecnologías de la información para ser competitivas en el mercado global y llegar a la mayor cantidad de clientes posibles. No obstante, en el desarrollo de su actividad comercial tratan grandes cantidades de datos personales de los clientes, mismos que deben ser protegidos cuidadosamente para garantizar la integridad física y patrimonial de las personas humanas, para tal efecto, la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* establece el marco normativo que da cumplimiento al artículo 16° de la *Constitución Política de los Estados Unidos Mexicanos,* mismo que reconoce el derecho a la protección de datos personales como un derecho humano, en la citada Ley se encuentran plasmados los principios rectores del tratamiento de los datos, así como la obligación de implementar las medidas de seguridad administrativas, técnicas y físicas, para garantizar la confidencialidad de los mismos ante terceros no autorizados. En tal sentido, el principal problema en el cumplimiento de dichos principios, recae sobre el desconocimiento jurídico y técnico, no en la ineficacia de la Ley en sí.


Palabras clave: Sociedad de la Información, derecho a la protección de datos personales, tratamiento de datos personales, cómputo en la nube, privacidad e intimidad.


## *ABSTRACT*

*The Mexican economy is supported mostly by micro-enterprises, in order to know the needs of the information society, should implement the use of information technologies to be competitive in the global market and reach as many customers as possible. However, in the development of their commercial activity they process large amounts of customers personal data, that must be carefully protected to ensure the physical and patrimonial integrity of human persons, for this purpose, the Federal Law on the Protection of Personal Data Held by Private Individuals establishes a*

*regulatory framework that complies with 16th article of the Political Constitution of the United Mexican States, that recognizes the right to the personal data protection as a human right, the aforementioned Law reflects the principles guiding of the data processing, as well as the obligation to implement administrative, technical and physical security measures, to guarantee the confidentiality of them before unauthorized third parties. In this sense, the main problem in the fulfilment of those principles lies with the legal and technical ignorance, not the ineffectiveness of the Law itself.*

*Keywords: Information Society, right to personal data protection, personal data treatment, cloud computing, privacy.*

# INTRODUCCIÓN

El presente trabajo se ha dividido en cuatro capítulos, el primero se aboca a los conceptos técnicos y abarca temas en los que se analiza de manera general como el desarrollo de las Tecnologías de la Información y Comunicación que se produjo en el periodo de la revolución industrial, dio como resultado la invención de grandes tecnologías, entre las cuales se destacan las computadoras. Así, partiendo de la creación de la UNIVAC *(UNIVersal Automatic Computer),* en el año 1951 como la primera computadora de propósito general que se fabricó en serie para su uso empresarial, se puede notar que la finalidad era la automatización de tareas en el procesamiento de información.

Este desarrollo tecnológico trajo consigo grandes beneficios para las empresas gracias al potencial que suponía esta nueva tecnología, pues gracias a ello las empresas podían ahorrar tiempo y dinero. Este suceso dio como resultado los primeros pasos hacia un nuevo paradigma en la forma de relacionarse y de hacer negocios, dando inicio a lo que hoy día se conoce como la sociedad de la información, una sociedad altamente influenciada por las tecnologías, que depende en gran medida de la tecnología para el desarrollo de sus actividades cotidianas.

Así entonces, las empresas que desean ser competitivas en el mercado global y mantenerse a la vanguardia, deben hacer uso de estas tecnologías, no obstante, tomando como contexto el caso de México donde las estadísticas del INEGI demuestran que el 97.6% de las empresas son microempresas y concentran el 75.4% del personal ocupado, es de entender que muchas de estas empresas no tengan ni el personal especializado para operar las tecnologías, ni el recurso suficiente para mantener los centros de cómputo que se requieren.

Por tal motivo, se ven obligadas a contratar servicios de cómputo en la nube según sus necesidades tecnológicas, sea software como servicio, plataformas como servicio o infraestructura como servicio en algunas de sus modalidades de despliegue, además, este tipo de aprovisionamiento tecnológico también posibilita el uso de tecnologías de *Big Data* e inteligencia artificial, útiles en el análisis de información con fines mercadotécnicos, y para la planeación de las actividades

futuras de la empresa, bajo la premisa de certidumbre que brindan estas tecnologías.

Por su parte, en el segundo capítulo se analizan temas relacionados a la naturaleza del derecho a la información, la protección de datos personales, así como la privacidad e intimidad, con la intención de comprender el origen del derecho a la protección de datos personales, su evolución y la relación con las tecnologías de la información y comunicación.

Este capítulo ayuda a comprender que el origen de este derecho, deriva del descubrimiento de *Internet* en los años 60's como medio para intercambiar información, aunado al potencial de las tecnologías de procesamiento de información –computadoras–, desveló una posible amenaza para la privacidad desde los años 70's; bajo esa preocupación se creó la primera ley sobre protección de datos personales en el Estado de *Hesse,* Alemania, en el año 1970 con la firme intención de limitar el uso de la informática, para garantizar la privacidad de las personas.

Posteriormente, en el año 1973, se crea en Suecia la que se podría considerar como la primera ley de protección de datos personales en el mundo, y a partir de ello se comienzan a crear otras leyes en torno a la protección de datos personales en otros países.

Así, en 1974 se crea en Estados Unidos la *Privacy Act,* siendo estas tres leyes las que originan el reconocimiento del derecho a la protección de datos personales en el mundo, y sobre las cuales se han basado la mayoría de las leyes subsecuentes que se han replicado en todo el mundo, bajo la premisa de garantizar la privacidad y la intimidad de las personas frente al uso de las nuevas tecnologías de la información.

Estas leyes cobran mayor relevancia después de que Tim Berners-Lee creara la *World Wide Web* (www) en el año 1989, desarrollo que, apoyado de Internet, harían realidad lo que se plasmó en la *Declaración Universal de los Derechos Humanos* de 1948 en el artículo 19, respecto a la difusión de información sin limitación de fronteras, ya que estas tecnologías trabajando al unísono, podían transmitir

información de manera global en tan solo unos segundos, además de poder acceder y recibir información de distintas partes del mundo.

Esto generó una preocupación global, por lo que se vio la necesidad de abundar en estudios jurídicos, éticos y sociales para mejorar las leyes de protección de datos personales, y gracias a los convenios de colaboración y los tratados internacionales, se logró establecer un marco regulatorio internacional en torno a los principios que rigen el tratamiento de datos personales, el cual opera bajo la premisa de la libre circulación de datos para el desarrollo económico de las naciones, con la garantía del respeto a la privacidad y la protección del Estado ante posibles violaciones al derecho a la protección de datos personales.

En tal sentido, esa libertad para la circulación transfronteriza de datos personales, resulta comprensible desde el punto de vista de la interacción humana en la sociedad de la información, donde para ejercer el derecho al libre desarrollo de la personalidad, requiere la libertad para relacionarse con otras personas e interactuar con las empresas en la economía digital. No obstante, la información que se refiere a la intimidad, entendida esta como la esfera más íntima donde converge información reservada para el entorno familiar y/o personal, no es necesario divulgarla para que la persona de desarrolle libremente en sociedad.

La divulgación de esta información que se considera sensible a la luz de las leyes de protección de datos personales, puede originar actos de discriminación o de violencia, motivo por el que se debe mantener confidencial ante terceros no interesados. Por otra parte, los datos que corresponden a las esferas del honor, la dignidad, la propia imagen y la reputación, deben circular de manera controlada por su titular, con la finalidad de que la persona pueda construir una identidad personal pública, ejerciendo su libertad personal y su libre autodeterminación informativa.

En la actualidad el uso de *Big Data* para la recolección de información y la inteligencia artificial para el análisis de la misma, ha incrementado el flujo de datos que circulan en *Internet* sin limitación de fronteras, lo que ha incrementado la necesidad de contar con una garantía por parte del Estado para proteger los derechos de las personas sin limitar el desarrollo de las actividades comerciales.

En tal sentido, México se sumó a los países que cuentan con una ley de protección de datos personales en posesión de los particulares hasta el año 2010, posterior al reconocimiento constitucional de este derecho en 2009. En dicha Ley se encuentran plasmados los ocho principios que rigen el tratamiento de datos personales en México, los deberes y obligaciones a los que se hace acreedor el responsable del tratamiento, las sanciones por el incumplimiento a lo establecido en la Ley, así como las excepciones a la misma.

En el tercer capítulo se realiza el análisis de los avisos de privacidad de diez empresas, con la intención de verificar el cumplimiento de la Ley ante el uso las tecnologías de comercio electrónico, las cuales suponen el uso del cómputo en la nube, así como los riesgos que supone para la privacidad el protocolo de resolución e nombres de dominio DNS y el protocolo de transferencia de hipertexto HTTP, lo que deja claro que, aunque la Ley mexicana, los tratados y convenios internacionales en materia de protección de datos personales de los que México es parte, establecen el marco normativo para la debida protección de este derecho, se ha podido constatar que las empresas siguen incurriendo en errores que violan los principios que rigen el tratamiento de estos datos.

Aunado a ello, las empresas que realizan comercio electrónico, por lo regular contratan servicios de nube para el tratamiento de los mismos, lo que da como resultado la transferencia internacional de datos personales, suceso que, en la mayoría de los casos no se da a conocer al titular de manera adecuada, ello parece deberse al desconocimiento de la forma en que operan las tecnologías y al desconocimiento de la Ley.

Además, la escasa regulación para las empresas que prestan este tipo de servicios tecnológicos, propicia la violación del derecho sin que el responsable tenga la posibilidad de evitarlo, concretamente se puede observar que el protocolo de resolución de nombres de dominio DNS (por sus siglas en inglés), facilita el perfilado de los usuarios en la red, información que puede dar origen a la identificación de la persona e incluso, el análisis de dichos patrones de consulta podría determinar información sensible inherente a la persona, sin que eso signifique que el responsable del tratamiento los utilice para fines propios.

Otro ejemplo que se relaciona con las medidas de seguridad y los protocolos de comunicación, el protocolo de transferencia de hipertexto HTTP (por sus siglas en inglés), del cual se puede extraer información confidencial que puede ser usada para vulnerar la seguridad de los sistemas, o para conocer los datos que se envían mediante formularios web a la base de datos donde se resguardan, sin haber implementado las medidas de seguridad técnicas apropiadas.

Por tal motivo, es necesario que los responsables adopten una cultura de preparación para que el personal que interviene en el tratamiento de los datos personales, conozca las Leyes, tratados y convenios internacionales, así como los procedimientos adoptados por la empresa para garantizar el respeto de este derecho.

En lo que respecta al cuarto capítulo, tiene como finalidad servir de guía de cumplimiento de la Ley para los responsables del tratamiento de datos personales, en el se presenta de manera general el contenido del documento de seguridad, el ejemplo de cómo realizar un análisis de riesgo y la implementación de medidas de seguridad administrativas y técnicas, así como los resultados proporcionados por el INAI referente a la imposición de sanciones.

En tal sentido, resulta de interés mencionar que la empresa responsable del tratamiento debe designar a una persona o departamento responsable de datos personales, según lo considere necesario para dar atención oportuna a las solicitudes de derechos ARCO, así como vigilar el cumplimiento de la Ley, e implementar medidas de seguridad físicas y administrativas, mantener actualizado el documento de seguridad y el análisis de riesgos, así como coordinarse con el departamento de tecnologías para determinar las medidas de seguridad técnicas a implementar.

Es importante detenerse a observar los datos proporcionados por el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, en relación a las sanciones que han resultado a consecuencia de procedimientos de protección de derechos, pues tan solo del 23 de junio de 2019 al 23 de junio de 2020, se han emitido 595 resoluciones en las que se han impuesto sanciones por el incumplimiento a los principios o disposiciones de la Ley, de las

cuales 275 han sido impugnadas ante las autoridades administrativas y/o federales, sin que se tenga el conocimiento del desenlace de las mismas.

En relación a las multas cobradas, el mismo INAI desconoce el número total puesto que, el órgano facultado para recaudar el dinero de las mismas, es el Servicio de Administración Tributaria (SAT), mientras que de manera voluntaria solo trece empresas han informado al instituto sobre tales efectos, dando un total de $51,719,498.87 pesos, lo que debe alertar sobre la importancia del cumplimiento de la Ley en el tratamiento de los datos personales.

Como medidas para evitar ser acreedores de sanciones por el órgano garante se proporcionan algunos parámetros técnicos y administrativos para la elaboración del documento de seguridad, se incluyen algunos elementos de importancia para determinar el análisis de riesgo en entornos de cómputo en la nube, los anexos que forman parte de las medidas de seguridad administrativas, y un plan de capacitación para el personal que desempeña funciones en la que traten datos personales, es importante precisar que el plan de capacitación que se propone puede variar dependiendo de las necesidades de la empresa. Sin embargo, se han considerado los temas que se cree aportan un panorama completo de los principios, deberes y obligaciones, así como el contexto general del derecho a la protección de datos personales.

*Estudia el pasado si quieres*
*intuir el futuro*

*- Confucio -*

# CAPÍTULO PRIMERO

## CONCEPTOS TEÓRICO–TÉCNICOS

### *1.1. Sociedad de la Información*

Mucho se ha dicho ya en diversas obras sobre la denominada 'sociedad de la información'. Sin embargo, analizando algunas de ellas, no queda claro a partir de qué fecha debe considerarse el inicio de la misma, pues para algunos se inicia desde la introducción de la tecnología para la automatización de los procesos de fabricación en el periodo de la Revolución Industrial, mientras que, para algunos otros, comienza desde el año 1962, a partir de una de las obras de Fritz Machlup[1]; algunos otros lo retoman a partir de 1996, cuando la UNESCO introdujo el concepto en el documento denominado: "La UNESCO y la sociedad de la información para todos"[2], y hay quienes retoman este concepto a partir de la Cumbre del Milenio de las Naciones Unidas en septiembre del año 2000[3].

Incluso el tema de sociedad de la información ha dado origen a la concepción de nuevas sociedades, como son, la sociedad del conocimiento[4] y la sociedad del aprendizaje[5]. Estos conceptos han llevado también a la concepción de conceptos como la economía de la información[6] y economía del conocimiento[7].

---

[1] Ileana R., Alfonso Sánchez, "La Sociedad de la Información, Sociedad del Conocimiento y Sociedad del Aprendizaje. Referentes en torno a su formación", *Reflexiones,* Núm. 2, Vol. 12, 2016, p. 236, https://dialnet.unirioja.es /descarga/articulo/5766698.pdf. Consultado: 15/09/2017.

[2] Cfr. UNESCO, *LA UNESCO y la sociedad de la información para todos,* 1996, https://unesdoc.unesco. org/ark:/48223/pf0000108540_spa. Consultado: 15/09/2017.

[3] Cfr. CEPAL, *La cumbre del milenio*, 2000, https://www.cepal.org/es/temas/objetivos-de-desarrollo-del-milenio-odm/acerca-odm. Consultado: 16/09/2017.

[4] Cfr. Avalos Rosado, Marco Carlos, *La sociedad del conocimiento*, San Luis Potosí, México, 2013, p. 5, https://static1.squarespace.com/static/51ede959e4b0de4b8d24e8a9/t/5213aa19e4b0750ce7ecb4c6/1377020441113/1.+La+sociedad+del+conocimiento.pdf. Consultado: 16/09/2017.

[5] Cfr. Stiglitz, Joseph Eugene y Greenwald, Bruce Corman Norbert, *La creación de una sociedad del aprendizáje,* Ediciones Cultrales Paidós, México D.F., 2014. Consultado: 19/09/2017.

[6] Cfr. Otter, Thomas y Mónica Cortez, *Economía de la Información, Sociedad de la Información, Información Periodística: Elementos compartidos hacia una información pluralista y equitativa*, Konrad-Adenauer-Stiftung, Lima, 2003, https://paisdospuntocero.files.wordpress.com/2015/04/18-kas_4901-1522-4-303.pdf.

[7] Cfr. Sánchez, Carlos y Humberto Ríos, "La economía del conocimiento como base del crecimiento económico en México", Enl@ce: *Revista Venezolana de Información, Tecnología y Conocimiento*, Núm. 2, Vol. 8, 2011, p. 46, https://www.redalyc.org/pdf/823/82319126004.pdf. Consultado: 20/09/2017.

No obstante, aunque estos términos han dado origen a numerosos estudios que tienen como objetivo sustentar la necesidad de un cambio de paradigma, que busca comprender las transformaciones sociales y los cambios en las mismas organizaciones comerciales que utilizan la información y la tecnología para hacer negocios, no debemos olvidar que, cuando se habla de una sociedad del conocimiento, sociedad del aprendizaje o de la misma economía de la información y del conocimiento, siempre se hace en relación a la información que se procesa o circula en medios electrónicos, lo que indica que todo gira en torno a la información; lo que cambia es el entorno de aplicación, ya sea en las empresas, en el sector social o el sector educativo.

Así entonces, partiendo de esta generalidad y basados en la premisa de que, al hablar de una sociedad de la información se entiende que es una sociedad ávida de información, en este estudio retomaremos el concepto de sociedad de la información a partir del año 1951, año en que se desarrolló la primera computadora de propósito general, la UNIVAC *(UNIVersal Automatic Computer)*, es decir, fue la primera computadora que podía ser usada para procesar información diversa, en ese sentido, esta nueva tecnología permitía la aplicación de la misma para el procesamiento de información administrativa, científica, médica, etc. Siendo su única limitante para la sociedad, el elevado costo de la misma.

Lo anterior es un referente puesto que, a partir de este desarrollo tecnológico comenzaron a aparecer otros descubrimientos que permitirían conectar dichas computadoras para poder compartir información, que si bien, la red de *Internet* surgió como una tecnología de aplicación militar, pronto se haría comercial por su potencial prometedor para el comercio y las comunicaciones civiles[8]

En ese sentido, se puede inferir que a partir de que las tecnologías de la información comenzaron a ser usadas para el procesamiento de todo tipo de información, agilizando las tareas de análisis para la toma de decisiones, comenzó el cambio de paradigma social, más que por el hecho de que la sociedad se base en el cúmulo de información con la que cuenta, es por la información que las

[8] Cfr. Kenneth C., Laudon y Guercio Traver, Carol, *E-commerce 2013. Negocios, Tecnologías y Sociedad,* Pearson Educación, México, 2014, p. 119.

organizaciones obtienen y procesan de la sociedad, con ayuda de las nuevas tecnologías.

Sin embargo, posteriormente las computadoras se fueron reduciendo tanto en tamaño como en costo, esto permitió que la sociedad tuviera la posibilidad de adquirir dichos artículos, ya no solo para uso empresarial, sino para uso personal. De esta forma, cada vez fueron más las personas que poseían una computadora personal para realizar diversas actividades que involucran el procesamiento de información.

Entonces, se puede aseverar que los conceptos de sociedad del conocimiento, sociedad del aprendizaje, economía de la información, economía del aprendizaje y economía del conocimiento, son términos que han sido acuñados para distinguir los sectores sociales en donde se aplican dichos conceptos. Sin embargo, argumentando a favor de la sociedad de la información, parece que el concepto de sociedad del conocimiento no tiene ningún sustento puesto que, el conocimiento surge de la información que los individuos pueden obtener de diversos medios y en cualquiera de los formatos perceptibles para el ser humano.

De igual modo, si hablamos de la sociedad del aprendizaje, parece que es un término usado en el contexto académico y empresarial. No obstante, volvemos a lo mismo, el aprendizaje se da mediante la transmisión de conocimiento por el emisor y la recepción de información por el receptor, esto se convierte en un ciclo que nos dirige siempre a la información que se percibe y procesa, sea en dispositivos electrónicos o por el cerebro humano, de donde se obtiene un conocimiento que, al momento de ser transmitido, se presenta a manera de información.

Lo mismo sucede en las empresas cuando el procesamiento de información da como resultado el conocimiento de sus clientes, la predicción de ventas, la probabilidad de éxito de un nuevo producto, etc. Consecuentemente, es notorio que el concepto de economía del conocimiento, no es más que un término utilizado para hacer referencia a la aplicación de la información por las empresas, pues por lo regular es usada para reducir el riesgo en los negocios y para emprender acciones basadas en el conocimiento derivado de la información con la que cuenten, lo que se traduce en una toma inteligente de decisiones.

No por nada la información se ha convertido en uno de los activos más valiosos para las empresas y el más codiciado por los rivales comerciales, e incluso para los grupos delictivos, pues con la información se aprende, es decir, se obtiene conocimiento y, por ende, genera ingresos para quien posee la información. No obstante, la relación entre la sociedad de la información y la tecnología son inseparables, pues sin la tecnología para procesar grandes cantidades de información, no se podría obtener el conocimiento necesario para generar economía, y sin la información, la tecnología no generaría el conocimiento que se requiere de la sociedad para brindar los satisfactores sociales, que por otro lado permiten la circulación de la economía de las naciones.

En virtud de lo anterior, puede argumentarse a favor de la 'sociedad de la información' como único concepto que engloba aprendizaje, conocimiento y mueve la economía, a partir de la proliferación de las tecnologías y con la llegada del *Internet,* la sociedad cada vez más, deja las tareas de recolección, procesamiento y análisis de la información a la tecnología, y por ende, la economía se mueve en torno a la cantidad de información que circula en la red.

Esto no necesariamente significa que la sociedad cuente con más información para la toma de decisiones, sino más bien, que gracias al *Internet* y a la cantidad de dispositivos tecnológicos que actualmente usa la sociedad, las personas generan mayor cantidad de información susceptible de ser procesada por y para las empresas, de la cual pueden obtener un beneficio económico.

Así, puede aseverarse que las personas, mediante el uso de tecnologías, generan grandes cantidades de información susceptible de ser procesada por las empresas, de la cual obtienen conocimiento para el desarrollo de satisfactores sociales. Así entonces, la relación entre sociedad de la información y el desarrollo económico es muy estrecha, pues el uso de las tecnologías de la información ha tenido como principal objetivo la competitividad en el mercado global, lo cual solo se puede lograr mediante la implementación de tecnologías de la información y comunicación para el aprovechamiento de la información.

En consecuencia, la necesidad de regular las actividades de recolección de datos personales por las empresas comienza a tomar sentido, ya que es notorio que por

la competencia en la que se desarrolla la actividad económica hoy en día, las empresas vulneren derechos humanos para posicionar sus productos en el mercado de la sociedad de la información, un mercado caracterizado por desplegar sus productos, además de en un espacio físico, en el ciberespacio, al que cualquier persona que se encuentre inmersa en dicha sociedad, podrá acceder sin limitaciones de lugar y tiempo.

Lo anterior queda limitado a las características de la población de que se trate, pues no olvidemos que la *brecha digital* es una limitante para lograr el aprovechamiento de las tecnologías de la información, dando como resultado una sociedad de la información fragmentada, acorde a las posibilidades económicas y de acceso a la conectividad –*Internet–,* siendo esto un factor negativo en el goce de los beneficios planteados para el desarrollo de la sociedad de la información.

En resumen, respecto a la unificación del concepto de sociedad de la información, se puede argumentar que la información genera conocimiento, el aprendizaje proviene del conocimiento de otros y se transmite a manera de información. Por su parte, la aplicación del conocimiento en algún sector comercial, genera retribución económica, esa retribución fluctúa en relación al grado de asertividad en la toma de decisiones basadas en la información con que se cuente respecto a un contexto específico y en la veracidad de la misma.

De tal manera que no tiene sentido hablar de denominaciones distintas de sociedad, si finalmente, estas están conformadas por: la sociedad, la información y la tecnología, elementos que dieron origen a la concepción de la sociedad de la información, y existe un vínculo estrecho entre estos elementos y los conceptos de conocimiento y aprendizaje. Se entiende, entonces, el resultado de su interacción como el aprovechamiento de la información que genera la sociedad, para el desarrollo económico y la competitividad empresarial en el mercado global.

### *1.2. Definición y concepto de MiPYME*

MiPYME es la nomenclatura para referirse las Micro, Pequeñas y Medianas empresas, por lo que se considera que no tiene relevancia ahondar en la definición del término. Sin embargo, sí es importante tener en cuenta el concepto de empresa,

ya que, sin importar su clasificación por tamaño de acuerdo con la nomenclatura, todas ellas operan bajo ciertas similitudes respecto a los recursos, métodos y estrategias mercadológicas, que finalmente las coloca dentro de alguna categoría.

Interpretando a Hernangómez[9] las empresas se conciben como una unidad económico-social que conjunta capital, trabajo, recursos materiales y humanos bajo una dirección que guía los esfuerzos para lograr los objetivos empresariales.

Para Chiavenato, la empresa "es una organización social que utiliza una gran variedad de recursos para alcanzar determinados objetivos [y explica que la empresa] es una organización social por ser una asociación de personas para la explotación de un negocio y que tiene por fin, un determinado objetivo, que puede ser el lucro o la atención de una necesidad social"[10].

Por su parte, Gerardo Bautista menciona que “una empresa es un grupo social, que, a través del capital, el trabajo y la administración, se producen bienes o distribución de bienes y servicios con fines lucrativos o no y tendientes a la satisfacción de las necesidades de la comunidad”[11].

Si bien la definición de empresa puede variar según el autor y la época, se mantiene su concepción como un ente económico-social, que reúne recursos materiales, económicos, tecnológicos y humanos para el desarrollo de una actividad específica con el objetivo de satisfacer necesidades sociales y económicas. Estos recursos deben concebirse como el sistema de la empresa, el cual requiere de la integración de todas las partes mencionadas para un correcto funcionamiento de la misma.

La clasificación de las empresas puede variar dependiendo del organismo que haga dicha clasificación y del país de que se trate; por ello es que en este trabajo no se hará un análisis a profundidad respecto a las distintas maneras de clasificar las empresas y solo se mencionarán algunas de ellas a manera de ejemplo. No

---

[9] *Cfr.* Hernangómez Barahona, Juan José, "La empresa como organización: una propuesta de delimitación de su concepto", *Anales de estudios económicos y empresariales,* núm. 3, 1988, https://dialnet.unirioja.es/servlet/articulo?codigo=785516. Consultado: 11/03/2018.

[10] Chiavenato, Idalberto, *Iniciación a la Organización y Técnica Comercial*, México, Mc Graw Hill, 1993, p. 4.

[11] Bautista Bautista, Gerardo, *Clasificación de las empresas en México*, Universidad Autónoma del Estado de Hidalgo, https://www.uaeh.edu.mx/scige/boletin/prepa4/n5/m14.html. Consultado: 15/10/2017.

obstante, es necesario señalar que cuando hablamos de empresas nos remitimos al artículo 3 de la *Ley Para el Desarrollo de la Competitividad de la Micro, Pequeña y Mediana Empresa*[12], en donde se definen como MiPYIMES las empresas legalmente constituidas.

Es importante señalar que la clasificación no representa en sí un cambio en la composición de los elementos que integran la empresa en función de su tamaño y sector en que se desarrolla la actividad, pero sí varía la productividad, el volumen de ventas y la contribución al desarrollo económico del país, a través la generación de empleos y la aportación al Producto Interno Bruto (PIB) mediante el pago de impuestos a la autoridad fiscal.

Aunque las empresas pueden clasificarse de distintas maneras, las más usuales en México son en función de su tamaño, giro, origen de su capital y el sector económico[13]. Sin embargo, para el caso que nos ocupa respecto a las MiPYMES, nos basaremos en el *Acuerdo por el que se establece la estratificación de las micro, pequeñas y medianas empresas*[14], derivado del artículo 3 fracción III de la *Ley Para el Desarrollo de la Competitividad de la Micro, Pequeña y Mediana Empresa*. En dicho acuerdo se hace una estratificación de las MiPYMES por tamaño, sector y volumen de ventas anuales, como se presenta a continuación en la tabla 1.1.

| **Estratificación** | | | | |
|---|---|---|---|---|
| **Tamaño** | **Sector** | **Rango de número de trabajadores** | **Rango de monto de ventas anuales (mdp)** | **Tope máximo combinado*** |
| Micro | Todas | Hasta 10 | Hasta $4 | 4.6 |
| Pequeña | Comercio | Desde 11 hasta 30 | Desde $4.01 hasta $100 | 93 |
| | Industria y Servicios | Desde 11 hasta 50 | Desde $4.01 hasta $100 | 95 |
| Mediana | Comercio | Desde 31 hasta 100 | Desde $100.01 hasta $250 | 235 |
| | Servicios | Desde 51 hasta 100 | | |

[12] Reforma publicada en el DOF el 19-05-2017, http://www.diputados.gob.mx/LeyesBiblio/pdf/247_190517.pdf. Consultado: 20/02/2018.
[13] *Cfr.* Hernández y Rodríguez, Sergio, *Introducción a la Administración*, México, McGRAW-HILL, 2011, pp. 8-9.
[14] Publicado en el DOF el 30-junio-2009, https://www.gob.mx/cms/uploads/attachment/file/50882/A539.pdf. Consultado: 20/02/2018.

| | | | | |
|---|---|---|---|---|
| | Industria | Desde 51 hasta 250 | Desde $100.01 hasta $250 | 250 |

Tabla 1.1. Estratificación de las micro, pequeñas y medianas empresas.
*Fuente: Diario Oficial de la Federacion.*

Cabe señalar que de acuerdo a la Ley, en la estratificación establecida "se incluyen productores agrícolas, ganaderos, forestales, pescadores, acuicultores, mineros, artesanos y de bienes culturales, así como prestadores de servicios turísticos y culturales", por lo que cuando nos referimos al sector económico, nos estamos refiriendo al sector prioritario para el desarrollo económico establecido en la Ley y no a los sectores primario, secundario y terciario como lo manejan algunos estudiosos de la administración.

De tal manera que con base en esta estratificación y tomando en cuenta las estadísticas, parece notorio que las MiPYMES son un eslabón de gran importancia para el desarrollo de la economía, pues la mayoría de las empresas existentes en México están dentro de esta clasificación y son las que generan mayor cantidad de empleos.

Esta afirmación se puede contrastar con datos consultados en el Instituto Nacional de Geografía e Informática (INEGI) que en el año de 1998 registra un número de MiPYMES en México "[…] de tres millones 38 mil 514 establecimientos a nivel nacional, el 95.4% de establecimientos estaba ocupado por microempresarios, el 3.3% por las pequeñas empresas, el 0.9% por las medianas empresas […]. Es decir, 3,027,518 […]"[15] en total, eran MiPYMES.

Según el boletín de prensa que dio a conocer el INEGI en julio de 2016, en el año 2014 existían en México 4'048,543 (cuatro millones, cuarenta y ocho mil quinientas cuarenta y tres empresas), de las cuales "[…] 97.6% son microempresas y concentran el 75.4% del personal ocupado total, seguidas por las empresas pequeñas con el 2.0% y el 13.5% y las medianas que representan el 0.4% y el 11.1%, respectivamente"[16]. Tal como se ilustra en la figura 1.1.

---

[15] Bárdan Esquivel, Cuitláhuac y Rivera Paz, Gustavo (coords.), *Micro, Pequeñas y Medianas Empresas en México. Evolución, Funcionamiento y Problemática,* México DF, Instituto de Investigaciones Legislativas del Senado de la República, 2002, p. 12.

[16] Instituto Nacional de Estadística y Geografía, *Boletín de Prensa Núm. 285/16*, Aguascalientes, 2016, p. 2. http://www3.inegi.org.mx/rnm/index.php/catalog/330/download/9792. Consultado: 10/03/2018.

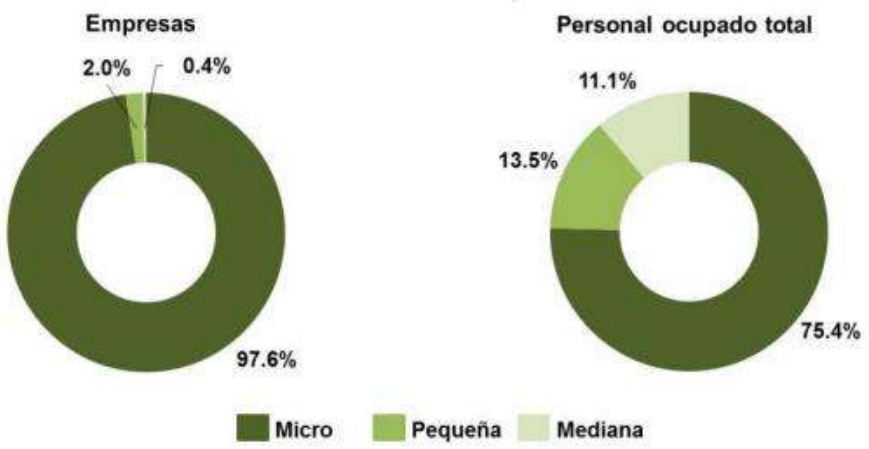



Figura 1.1. Distribución del número de empresas y del personal ocupado total por tamaño de empresa, 2014
*Fuente: BOLETÍN DE PRENSA NÚM. 285/16. INEGI*

Si se observan las estadísticas a través del tiempo, no han cambiado considerablemente de 1998 hasta 2014, así entonces, resulta evidente que la economía mexicana se halla soportada mayormente por las microempresas, mismas que en la mayoría de los casos se encuentran en desventaja competitiva en el mercado global contra las grandes empresas que cuentan con los recursos económicos suficientes para la integración de tecnología especializada, la contratación de personal altamente capacitado para administrar los recursos de la empresa y lograr cierto control del mercado. Sin embargo, las MiPYMES siguen siendo las de mayor importancia para el desarrollo económico de México.

Debido a esta desventaja de recursos económicos que les permita adquirir la tecnología y contratar al personal especializado para su operación, muchas microempresas optan por contratar los servicios de cómputo en la nube para el desarrollo de su actividad económica, servicios que son utilizados para diversos fines que van desde la facturación electrónica mediante servicios que se adquieren en modalidad de nube, hasta la puesta en marcha de un sistema de comercio electrónico o el despliegue de un sitio web para promocionar los productos o servicios de la empresa.

Estos servicios suponen un ahorro en la inversión en tecnología, ya que no es necesario adquirir los equipos especializados ni pagar personas adicionales para

que las opere, por ello es que este tipo de servicios de cómputo en la nube ha tenido una gran aceptación en el sector empresarial y más aún en las micro empresas.

Por ello, es importante mencionar que, conforme a la clasificación anterior, las MiPYMES están identificadas no solo por su tamaño, sino también por el sector en el que desarrollan su 'actividad económica'[17]. Esto es importante para el análisis debido a que, dependiendo del sector cambiará la estrategia administrativa implementada para sobresalir en la competencia global del mercado en el que se desenvuelve la empresa, pues no en todos los sectores existe el mismo grado de competencia y, por ende, se requiere de la integración de distintas tecnologías.

Así entonces, basados en la *Ley para el Desarrollo de la Competitividad de la Micro, Pequeña y Mediana Empresa*, se identifican las empresas de acuerdo al tamaño y a los sectores económicos, dividiéndose en Industria, Comercio y Servicios, como se ilustra a continuación en la tabla 1.2.

| **Sector/Tamaño** | **Industria** | **Comercio** | **Servicios** |
|---|---|---|---|
| Micro | 0-10 | 0-10 | 0-10 |
| Pequeña | 11-50 | 11-30 | 11-50 |
| Mediana | 51-250 | 31-100 | 51-100 |

Tabla 1.2. Estratificación por número de trabajadores
*Fuente: Ley para el Desarrollo de la Competitividad de la Micro, Pequeña y Mediana Empresa. Art. 3. Fracción III.*

De acuerdo al boletín de prensa dado a conocer por el INEGI, el sector comercio está representado por un 56.5% de empresas y un total de personal ocupado de 48.2%, "[…] por debajo de dicho sector se encuentran los servicios que registraron un 32.4% del total de empresas y un 32.9% del personal ocupado […]"[18], las empresas industriales o manufactureras ocupan un 11.1% con un 18.9% de personal ocupado, tal como se muestra en la figura 1.2.

[17] Se retoma la siguiente definición de 'actividad económica': "Es el conjunto de acciones realizadas por una unidad económica con el propósito de producir o proporcionar bienes y servicios que se intercambian por dinero u otros bienes o servicios". Instituto Nacional de Estadística y Geografía, *Clasificación de las Actividades Económicas*, s.f., p. 2. http://www3.inegi.org.mx/rnm/index.php/catalog/205/download/5998. Consultado: 03/10/2019.
[18] Instituto Nacional de Estadística y Geografía, *Op. Cit.,* p. 6.

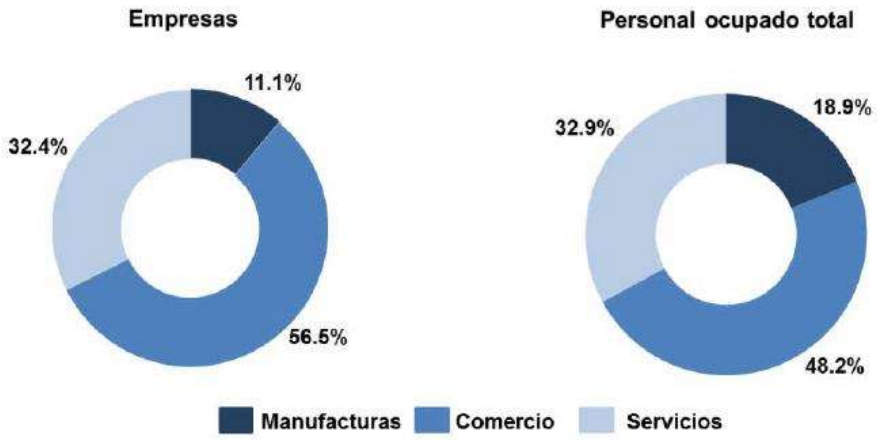



Figura 1.2. Distribución del número de empresas y del personal ocupado total por tamaño de empresa, 2014
*Fuente: BOLETÍN DE PRENSA NÚM. 285/16. INEGI*

Si bien es cierto que desde la doctrina de la administración es posible subdividir los sectores económicos en primarios, secundarios y terciarios, y cada uno de ellos a su vez en distintos tipos de industria, para este estudio solo se toman para su descripción los sectores prioritarios establecidos en la Ley, ya que de ello depende también el tipo de datos personales que son tratados por la empresa. No olvidemos que en México las empresas no gozan del derecho a la protección de datos personales.

De tal manera que las empresas que desarrollan su actividad económica en el sector industrial y distribuyen sus productos a otras empresas del sector comercial, tratan una menor cantidad de datos personales que aquellas empresas comercializadoras de productos y servicios. Por ello la importancia de identificar los sectores económicos.

De este modo, las empresas que desarrollan su actividad económica en el sector del comercio, son aquellas que enfocan sus esfuerzos a la compraventa de productos; esto significa que no son fabricantes de los productos que comercializan. De cierta manera, esto permite que la empresa pueda poner al alcance del público en general, mayor diversidad de productos de los que sería capaz de producir y vender una sola empresa por la complejidad que representa la producción de cada uno de los artículos existentes en el mercado.

La característica de los bienes que se comercializan en este sector, es que a cambio del pago por la compra de algún producto, el cliente se lleva un objeto físico que se traduce en un bien tangible y negociable, el cual puede ser un bien duradero o consumible según la característica del producto y acorde a la necesidad social a satisfacer con dicho producto.

Por su parte, el sector industrial está conformado por las empresas que se dedican a la transformación de materias primas a partir de las cuales elaboran nuevos productos que serán comercializados por las empresas del sector comercial. Los productos que elaboran estas empresas son bienes tangibles que pueden ser duraderos o consumibles.

Aunque es un número de empresas más reducido que el que conforma el sector comercial, es un sector trascendental para el desarrollo económico del país, ya que son las empresas que cuentan con mayor conocimiento para la conservación y transformación de las materias primas, lo que permite que mediante procesos especializados se puedan conservar los alimentos que sin un tratamiento adecuado no podrían ser exportados fuera del país, a la vez que son las empresas proveedoras del sector comercial.

Cabe señalar que los clientes de este tipo de empresas son las empresas del sector comercial, por lo que los datos personales que puede tratar se reducen a un número menor que el que pueden tratar las del sector comercial que realizan venta al público en general de manera física y/o en línea.

El sector de servicios se caracteriza por no comercializar con productos o bienes tangibles, sino por prestar servicios que satisfacen las necesidades de la sociedad; es un sector más pequeño que los dos anteriores, sin embargo, es tan necesario como cualquiera de los otros, ya que estas empresas se dedican a resolver problemas en cualquiera de los anteriores, así como de la sociedad en general.

La actividad que desempeñan estas empresas es la de prestar un servicio que pueda solucionar problemas desde la falla de un equipo especializado, hasta la prestación de un servicio que pudiera parecer insignificante, pero que finalmente satisface la necesidad de una persona o un grupo de personas.

Los bienes que se adquieren a cambio del pago de un servicio son consumibles e intangibles, es decir, que solo se disfrutan o satisfacen una necesidad. Por ejemplo, el servicio de telefonía que se paga mensualmente no se puede contemplar, solo se puede utilizar para satisfacer la necesidad de comunicación de mensajes auditivos, audiovisuales, gráficos y textuales, pero no es un servicio que pueda tocarse físicamente.

Los clientes de estas empresas no están limitados por el sector, sino que pueden prestar sus servicios a cualquiera de los sectores mencionados o al público en general, lo que les da un campo más amplio de actuación, pero que a la vez su actividad está menos valorada por los otros sectores y por lo general se enfocan a prestar sus servicios a la sociedad en general.

Estos tres sectores conforman el total de la actividad comercial de las MiPYMES, por lo que se consideran empresas de gran importancia para el desarrollo económico del país, sin embargo, requieren, además de conjuntar los recursos materiales, económicos y tecnológicos, tener los recursos humanos que hagan funcionar los demás recursos integralmente como un sistema empresarial.

Estas tareas administrativas en la actualidad no se conciben sin el apoyo de la tecnología, por lo que, independientemente de su tamaño, las empresas deben incorporar a sus procesos productivos, administrativos y mercadológicos las tecnologías de la información, con la finalidad de ser competitivos en el mercado global, llegando cada vez a más personas sin limitación de lugar y tiempo y, simultáneamente, mantener un acercamiento con los clientes que redunde en una lealtad a la empresa y les haga sentir una satisfacción más allá de la que un simple producto puede brindar al usuario final.

Esto puede hacer que las micro empresas poco a poco se vayan abriendo terreno en el mercado. Para ello es necesario conocer a los clientes y a los posibles clientes más que solo por un nombre o un número, sino conocer sus gustos, sus intereses e incluso sus posibilidades económicas y los lugares que frecuentan.

Esto es posible gracias a las nuevas técnicas de *Big Data* para la recolección y análisis de información de la actividad del usuario mientas navega en *Internet*, lo cual se logra mediante códigos informáticos incrustados en las cookies de la página

de la empresa, que al descargarse en la computadora permite hacer un monitoreo de los hábitos de navegación del usuario, a menudo, con fines publicitarios.

Aunado a ello, la tecnología de Inteligencia Artificial puede ir más allá con el análisis de la información recolectada, ya que puede incluso llegar a predecir los hábitos de compra, lugares que visitará la persona, etc. En otras palabras, permite estar un paso adelante del cliente.

Con base en la información recolectada y analizada mediante la implementación de técnicas de *Big Data* e Inteligencia Artificial, la empresa podría adquirir, producir y distribuir sus mercancías en los tiempos y lugares que resulten oportunos de acuerdo a los hábitos de los clientes, aumentando con ello las probabilidades de venta, optimizando las materias primas, disminuyendo la inversión en producción, reduciendo sus inventarios y aprovechando al máximo sus recursos.

Si de servicios se trata, mediante estas tecnologías es posible desplegar publicidad focalizada en ciertas zonas geográficas, para determinados gustos, intereses, grupos sociales o edades, actividades que se logran mediante la contratación de publicidad por campañas o por la compra de palabras en los buscadores.

Por ello es que la información se ha convertido en uno de los activos más valioso de las empresas, ya que con base en ello es que pueden tomar decisiones con base en conocimiento de hechos o en base a predicciones derivadas del análisis de la información con la que cuenten.

Estas tecnologías y técnicas aplicadas al sector empresarial, les da una gran ventaja competitiva frente a las empresas que no han incorporado aún la tecnología como parte de su proceso administrativo.

Como se ha dicho en torno a la sociedad de la información, la economía de los países gira en torno a la información, así "[…] la adopción de modelos de Administración del Conocimiento representa la clave del éxito de las empresas[19] […]". De esta manera, el conocimiento que se obtiene de la información es

[19] García Hernández, Sonia, "Inteligencia de Negocios para Incrementar la Competitividad en MiPYMES", en Alma Yunuen Arreola Talavera *et. al.* (coords), *Competitividad Global a Través del Emprendimiento e Innovación*, Morelia, CONLAMI-Universidad Michoacana de San Nicolás de Hidalgo, 2018, pp. 624-645.

aprovechado como una ventaja competitiva a favor de la empresa, llegando así a la denominada "economía de la información"[20], en donde se asevera que las empresas están ante una nueva forma de hacer negocios y que el éxito de las mismas en esta nueva era de la información depende en gran medida del uso que hacen de los datos con los que cuenta la empresa.

Desde esta perspectiva, la inversión en tecnología es indispensable para el crecimiento de la economía del país, ya que como hemos visto, las MiPYMES representan la mayor parte de las empresas de México y generan gran parte de los empleos, de forma que hacen aportaciones considerables al PIB. Así, se considera necesario que estas empresas adopten la tecnología para que incursionen en los modelos de administración basados en el conocimiento, el cual se deriva del análisis de la información que se recolecta mediante tecnologías.

No obstante, cabe señalar que estas técnicas de recolección y análisis de datos pueden poner en riesgo la intimidad de las personas, violentando sus derechos humanos y, por ende, poner en riesgo la estabilidad financiera de la empresa en caso de ser sancionada como resultado de una demanda por el mal uso de la información tratada en sistemas informáticos.

En ese sentido, es importante generar al interior de las empresas una cultura tecnológica y de respeto a los derechos humanos, para que los administradores de las mismas puedan integrar la tecnología en los procesos administrativos sin vulnerar los derechos, permitiendo que sean los mismos clientes quienes decidan si están dispuestos o no a que su información sea tratada por las empresas para los fines que le hayan sido informados mediante el aviso de privacidad.

### *1.3. Concepto de cómputo en la nube,* Big Data *e inteligencia artificial*

Como ya se ha dicho anteriormente, las empresas que desean sobresalir y ser competitivas en el mercado global y ante la competencia tecnológica que supone la economía de la información, las empresas han tenido que adoptar nuevas técnicas de recolección y análisis de la información, así como agilizar los procesos

[20] *Cfr.* Turner, Colin, *E-conomía de la información*, Bilbao, España, Ediciones Deusto, S.A., 2001.

administrativos, de producción y de distribución de los bienes y servicios que comercializan en sus respectivos sectores económicos.

La adopción de las tecnologías de la información, deben ser utilizadas de manera adecuada para hacer eficientes los procesos y obtener el máximo provecho de los recursos de la empresa. Sin embargo, el mal uso de las mismas o la operación de manera desinformada, puede derivar en repercusiones que pueden ir desde el desprestigio hasta las sanciones por las leyes vigentes aplicables, según corresponda de acuerdo a las afectaciones causadas a terceros.

Las tecnologías que pueden ser utilizadas como aliadas de las empresas van desde la contratación de servicios de cómputo en la nube que permiten tener sistemas administrativos en línea, sitios web de publicidad hasta tiendas en línea, sin tener que invertir en servidores y en personal que se encargue de la seguridad de la información y del óptimo funcionamiento de los equipos tecnológicos.

De igual manera, estos servicios representan una reducción de recursos financieros para la empresa puesto que, al no tener equipo especializado, se reduce el gasto por concepto de sueldos y salarios, mantenimiento y reparaciones de los equipos, así como el consumo de energía por la operación de los equipos especializados como pueden ser servidores de bases de datos o servidores de producción.

De tal manera que las compañías que ofrecen los servicios de cómputo en la nube, han ido evolucionando sus servicios con la finalidad de satisfacer el total de las necesidades, tanto de las empresas como de la sociedad en general; avances que han permitido la creación de "[…] tecnologías como, *grid computing*, *clusters computacionales*, *virtualización*, *web services*, y arquitectura orientada a servicios […]"[21], tecnologías que dieron paso a la llegada del cómputo en la nube, superando el concepto de *utility computing*[22].

El *cloud computing*[23], como se denominó en el idioma inglés en un principio debido al país donde se comenzó a desarrollar y a difundir esta tecnología, comenzó

[21] Arias, Ángel, *Computación en la Nube*, 2a. ed., Lexington, KY, USA., s.e., 2019, p. 9.
[22] Según Angle Arias, "*Utility computing* es un enfoque en el que los servicios son ofrecidos bajo demanda, de la misma forma que la electricidad y telecomunicaciones". *Idem.*
[23] *Cfr.* Joyanes Aguilar, Luis, *Computación en la Nube,* México DF, Alfaomega, 2012, p. 10.

a tomar importancia a partir del año 2008, cuando las grandes empresas tecnológicas comenzaron a difundir el advenimiento de una nueva tecnología, que prometía grandes beneficios para las empresas y que a su vez representaba un nuevo paradigma para la computación como se conocía hasta ese momento.

Se prevé que esta tecnología tendrá una relevancia tan importante como la propia web, pues los servicios que se ofrecen en modelos de computación en la nube se reciben mediante plataformas web, por lo que se requiere tener acceso a *Internet* para poder utilizar dichos servicios los cuales son recibidos de la misma manera en la que se recibe el suministro de electricidad, modelo de cómputo en donde está disponible en el momento que se requiere, por el tiempo que se requiera y solo se paga por el consumo de los recursos tecnológicos utilizados.

En un intento por encontrar la definición de cómputo en la nube, diversos autores, empresas tecnológicas y estudiosos del tema, han dado su definición, coincidiendo en que esta tecnología es un nuevo modelo de cómputo en el que los usuarios contratan los servicios con los proveedores, pudiendo utilizar recursos como infraestructura (servidores), plataformas (entornos de desarrollo) o aplicaciones (ERP's o de oficina).

Así entonces, la definición de computación en la nube o *cloud computing* según Ángel Arias, es "[…] un sistema de computación distribuido orientado al consumidor, que consiste en una colección de ordenadores virtualizados e interconectados, que son suministrados dinámicamente y presentados como uno o más recursos computacionales unificados […]"[24], es decir que los servicios de cómputo en la nube son diversos y prestados por distintos equipos que unen capacidades de cómputo y recursos para soportar la demanda de los usuarios. El usuario final recibe un servicio único como si se tratara de un equipo de cómputo local, aunque en realidad esté utilizando diversos recursos tecnológicos.

Por su parte el NIST (*National Institute of Standards and Technology*), define el cómputo en la nube como, "[…] un modelo que permite, convenientemente, el acceso bajo demanda a redes ubicuas para compartir un conjunto configurable de

[24] Arias, Ángel, *Op. Cit*. p. 13.

recursos de computación […], que se pueden proveer y liberar rápidamente con un mínimo esfuerzo de administración o interacción del proveedor del servicio"[25].

Agustín González comenta que la computación en la nube "[…] es que los recursos y servicios informáticos, tales como infraestructura, plataforma y aplicaciones, son ofrecidos y consumidos como servicios a través de la *Internet* sin que los usuarios tengan que tener ningún conocimiento de lo que sucede detrás"[26].

Bajo este modelo de cómputo en la nube, al no tener que adquirir equipos costosos y que requieran de conocimiento especializado para ser operado, las empresas pueden ahorrar en infraestructura tecnológica y canalizar sus esfuerzos humanos al logro de los objetivos de la empresa, haciendo uso de la nube y de otras tecnologías para el análisis de información, de la cual derivan las estrategias mercadotécnicas para la permanencia y competitividad en el mercado.

En todo caso, las empresas finalmente solo son propietarias de la información con la que cuentan en los sistemas de nube; la tecnología le pertenece al proveedor del servicio, por lo que las empresas operan en base al conocimiento derivado de la información que poseen, la cual está alojada en sistemas contratados bajo un modelo de *outsourcing* tecnológico en donde el servicio prestado es un espacio de almacenamiento, un servidor o una red que permite que la empresa opere y obtenga las ventajas tecnológicas necesarias para posicionarse como una empresa vanguardista en la era de la información y el conocimiento.

A esta diversidad de tecnologías de las cuales se puede hacer uso en la actualidad para hacer negocio basados en el conocimiento derivado de la información, es a lo que Turner le ha llamado la economía de la información. Tecnologías como *Internet*, computadoras, aplicaciones, recolección y análisis de información mediante algoritmos, inteligencia artificial y redes neuronales, permiten que las empresas aprovechen la tecnología para el procesamiento de información que les permita guiar sus acciones hacia el objetivo empresarial y lograr el posicionamiento en el mercado global.

---

[25] Primorac, Carlos R., *Computación en Nube*, Universidad Nacional del Nordeste, 2014, p. 5.
[26] González, Agustín, *Computación en la Nube*, Universidad Técnica Federico Santa María, 2009, p. 3. http://profesores.elo.utfsm.cl/~agv/elo322/1s09/project/reports/ComputacionEnLaNube.pdf. Consultado: 15/03/2019.

Según Turner “resulta evidente que cuando este mercado madure, las ventajas competitivas para las empresas y para la economía en su conjunto comenzarán a ser aprovechadas a fondo”[27]. Y menciona que esto “[…] tendrá un gran impacto en las estrategias empresariales en tanto que las empresas pretenden mantener su posición de competitividad ante este tipo de cambios”[28], que representa el avance tecnológico y la madurez de la economía de la información.

Por consiguiente, las empresas que desean estar a la vanguardia deberán implementar distintas tecnologías, las cuales deben “[…] abarcar la mayoría de aspectos empresariales, desde el conocimiento esencial sobre proveedores hasta el cliente especializado y el conocimiento del producto”[29].

Ante la implementación de estas tecnologías que tienen como principal objetivo la recolección, procesamiento, almacenamiento y análisis de información; el principal componente de riesgo es la seguridad de la misma, pues toda información que puede ser accedida desde *Internet* se ve vulnerable ante ataques cibernéticos, que pueden ir desde la simple denegación del servicio impidiendo el acceso a la información, hasta el daño (eliminación, alteración o encriptación) o el robo de la misma para fines delincuenciales, acciones que pueden poner en riesgo no solo la economía de la empresa, sino también la integridad física de las personas de quienes se posee información en los sistemas informáticos en la nube.

Sin embargo, poco a poco la economía de la información se convierte más en una realidad; basta señalar que las nuevas monedas digitales como el *bitcoin*, son en realidad un producto tecnológico resultado de la aplicación del conocimiento obtenido de la información y que se ha convertido en un nuevo producto. No obstante, es una moneda digital (basada en información) que permite hacer transacciones y que ha sido aceptada por la mayoría de los negocios como efectivo circulante en esta economía de la información, o como lo llamaría yo, (la economía digital).

En la economía digital, es posible afirmar que, cada vez nos encontramos con más productos intangibles, los cuales en realidad no sabemos su ubicación física,

[27] Turner, Colin, *Op. Cit*., p. 25
[28] *Ibidem*, p. 27
[29] *Ibidem*, p. 30

por ejemplo, los libros digitales por los que pagamos pero que realmente no sabemos dónde están almacenados, o la compra de *bitcoins* que no podemos tocar pero que nos sirven para comprar algunas cosas.

Todo esto realmente es un bien que genera un sentimiento de satisfacción basada solo en el conocimiento de la existencia del bien (el saber que poseemos algo), aun cuando no se pueda tocar, lo que se convierte en una posesión digital derivada de la evolución de las tecnologías para el procesamiento y tratamiento de la información que permitió obtener el conocimiento para evolucionar en una nueva economía: la economía digital.

Esto hace evidente la necesidad de incorporar tecnologías como *Big Data* para la recolección de información, Inteligencia Artificial para analizarla y obtener conocimiento (sabiduría) para el desarrollo de estrategias de mercado eficientes, y la nube para tener dicha información disponible desde cualquier lugar, en todo momento y accesible desde cualquier dispositivo capaz de conectarse a *Internet*, convirtiendo así la información en conocimiento, el conocimiento en estrategia y la estrategia en una nueva forma de hacer negocios; lo que se ha convertido en el pilar que sostiene la nueva economía basada en el conocimiento, la realidad actual de la economía mundial.

### *1.4. Cómputo en la nube,* Big Data *e inteligencia artificial*

Aunque estas tecnologías no son del todo recientes, es un hecho que en los últimos años han tomado mayor importancia, en parte, parece deberse a la necesidad por obtener un mayor beneficio de los elementos que, como ya se ha mencionado anteriormente, conforman la denominada sociedad de la información.

En ese sentido, es evidente que la tecnología de cómputo en la nube es de vital importancia, pues a través de ella, las empresas pueden instalar y desplegar sus sistemas o servicios mediante *Internet,* sin tener que realizar grandes inversiones en tecnología especializada, logrando presencia en el mercado global con una inversión acorde a sus necesidades tecnológicas, beneficiándose además de la seguridad que el proveedor brinda por el mismo costo de la prestación del servicio.

De igual manera, el *Big Data* o los datos masivos traducido al español, es una tecnología de suma importancia para la recolección y análisis de información, lo que permite a las empresas hacerse de nuevos conocimientos derivados del cúmulo de información a la que se puede tener acceso en la red. En otras palabras, esta tecnología permite extraer de entre una cantidad enorme de datos, solo aquellos que pueden ser relevantes para la empresa, con la intención de conocer el panorama del mercado con respecto a su oferta comercial, y en su caso, reorientar las acciones para ser competitivos en el mercado.

Por su parte, la inteligencia artificial es una de las tecnologías que ha dado más de que hablar por el impacto que ha tenido en diversos ámbitos, que van desde los asistentes personales hasta los sistemas de impartición de justicia, es una tecnología en la que se ha trabajado con miras a replicar el cerebro humano, a lo que se le han llamado redes neuronales. Las pretensiones de esta tecnología son poder llegar a desarrollar una inteligencia autoconsciente, que pueda actuar de la misma forma que los humanos, y que pueda estar al servicio de la humanidad en diversas actividades, desempeñando incluso funciones de alta especialización en áreas como la medicina.

Esta tecnología se ha presentado en los últimos años como la nueva promesa del mejoramiento de la calidad de vida de las personas. Sin embargo, de acuerdo a las pretensiones de la misma, también se torna en una tecnología muy propicia para la violación de los derechos humanos, sobre todo, el derecho a la protección de datos personales y a la intimidad.

No obstante, parece que por más que se haya avanzado en el desarrollo de esta tecnología, aún está lejos de llegar a replicar las funciones del cerebro, pues no deja de ser una tecnología basada en circuitos eléctricos, que si bien, aprende de la información a la que se le dé acceso, carece de sentimientos que le doten de capacidades empáticas para actuar de manera consciente ante determinadas circunstancias, pues en su lugar, actuará con base en resultados de operaciones de matemáticas computacionales como: cálculo de predicados, lógica binaria, álgebra booleana, por mencionar algunos.

### *1.4.1. Cómputo en la nube*

Cuando la información no se encuentra disponible en el momento exacto, de la manera correcta y sintetizada bajo los requerimientos precisos que permitan la toma de decisiones inteligentes basadas en un conocimiento, la finalidad para la cual ha sido recolectada y almacenada esa información pierde el sentido de utilidad; pasando de ser una inversión que genere utilidad, a un gasto sin retribuciones para la empresa.

Partiendo de esta idea, las grandes empresas de tecnología han evolucionado sus servicios con la premisa de mantener la información disponible para su consulta y actualización, las 24 horas del día, los 7 días de la semana durante los 365 días del año (24/7/365), haciendo uso de las bondades que el *Internet* representa para la accesibilidad sin limitaciones de lugar y tiempo.

Así entonces, las grandes empresas como *Microsoft*, *Amazon*, *Salesforce*, *Google*, *IBM*, *HP*, *Oracle* y *SAP*, por mencionar algunos, han desarrollado tecnología bajo la modalidad de cómputo en la nube para satisfacer las necesidades empresariales, ofreciendo una variedad de servicios a los que se puede acceder bajo demanda y pagando solo por lo que se consuma, tal como se haría con la electricidad o el agua potable.

No olvidemos que, tanto el suministro eléctrico como el de agua potable tienen un costo mínimo de operación y un adicional según el consumo del periodo. Sucede lo mismo con los servicios de cómputo en la nube, ya que, al hablar de un servicio bajo demanda, en el cual se paga solo por lo utilizado, no significa que no se deba pagar una tarifa fija, sino más bien, significa que, de acuerdo a las necesidades del usuario, puede aumentar o disminuir su plan contratado, configurando los servicios según sus necesidades, pagando solo por los servicios que requiere para operar.

Actualmente con la tecnología de la nube es posible solventar todas las necesidades tecnológicas de una empresa, gracias a las nuevas tecnologías desarrolladas para ser soportadas por diversos sistemas operativos que van desde equipos de escritorio hasta dispositivos móviles, permitiendo realizar trabajos en oficina y en campo, con la característica de poder administrar la información desde una misma conexión remota.

Desde su origen, esta tecnología se ha presentado como un modelo de negocio tecnológico que beneficia a las empresas y, a su vez, integra un componente de impacto medioambiental; reduciendo la emisión de gas carbónico generado por el consumo de energía eléctrica, el cual según estudios de *Gartner Group* representa un total del 2% de la emisión de este gas en el planeta, equivalente a la emisión del transporte aéreo, pero con una perspectiva de incremento mucho mayor[30].

Esto se logra mediante nuevas tecnologías embebidas en el *hardware* que permiten que el consumo energético sea bajo demanda, es decir, los *data center* donde se alojan los servidores que proporcionan los servicios de aplicaciones y almacenamiento en la nube, han incorporado tecnología de *hardware* que permite la administración del consumo energético, de manera que cuando el procesador no se encuentra ocupado a su máxima capacidad, el consumo de energía será menor y, conforme se incremente el requerimiento de poder de cómputo, también se incrementará el consumo de energía, permitiendo la correcta operación del *hardware*.

De igual manera los sistemas operativos han incorporado funciones de administración de energía disminuyendo las llamadas a recursos de *hardware* o inhabilitando en su totalidad los componentes cuando sea pertinente, disminuyendo con ello el consumo de energía.

Así mismo, las grandes empresas de tecnología que proveen servicios en la nube han optado por convenir con otras empresas para utilizar su infraestructura bajo demanda, es decir, en el momento que los recursos de un proveedor no son los suficientes para satisfacer la demanda de poder de cómputo o el espacio de almacenamiento, pueden hacer uso de los recursos de otra empresa que cuenta con dichos servicios sin que el usuario final se vea afectado. A esta administración tecnológica y energética se le ha denominado tecnología verde.

Esto permite que los usuarios (empresas) cuenten con los servicios necesarios para satisfacer el total de sus requerimientos sin limitaciones, aun cuando la empresa con quien se haya realizado el contrato de prestación de servicios no cuente con la infraestructura suficiente para ello, solventando estas limitantes con

[30] *Cfr.* Arias, Ángel, *Op. Cit*. p. 20.

la tecnología adecuada para hacer uso de servicios de nube de otro proveedor sin que se afecte el servicio que el usuario contratante recibe.

Estas son algunas de las ventajas que tiene para las empresas y el medio ambiente la tecnología de cómputo en la nube, a diferencia de la adquisición de tecnología propietaria, las cuales representan un consumo de energía por el sistema de enfriamiento, así como para mantener los servidores en operación, que aun cuando no se estén utilizando a su máxima capacidad, sí representan un consumo mayor por toda la infraestructura que se requiere para su operación y aseguramiento de la información.

Esto constituye así buena opción para las micro, pequeñas y medianas empresas: la contratación de servicios de cómputo en la nube, los cuales tienen impacto en la reducción de costos para la empresa e impacto positivo para el medio ambiente. Sin embargo, pese a las buenas medidas de seguridad que los proveedores han implementado para brindar seguridad e integridad a la información, no es posible garantizar la seguridad en un 100% debido a los tipos de servicios que pueden ser contratados y a los permisos que el proveedor proporciona al usuario para la administración de dicha tecnología.

Por ello, la principal preocupación que deriva de la implementación de tecnología de cómputo en la nube en las empresas, es la seguridad de la información, que a su vez representa un riesgo para la integridad física de los titulares de los datos personales que pueden ser tratados por las empresas en los diversos servicios que se ofertan en esta modalidad de tecnología.

*A. Características esenciales del cómputo en la nube*

En párrafos anteriores ya se han mencionado algunas de las ventajas que el cómputo en la nube propone para la puesta en línea de diversos servicios, los cuales pueden ser accedidos desde cualquier lugar en donde se tenga una conexión a *Internet*, así como la ventaja para el medio ambiente al reducir las emisiones de gas carbónico, no obstante, el NIST[31] define cinco características esenciales referentes

[31] *Cfr.* National Institute of Standards and Technology, *NIST Cloud Computing Standards Roadmap*, 2013, p. 8, [version impresa] doi: http://dx.doi.org/10.6028/NIST.SP.500-291r2. Consultado: 11/05/2018.

a: autoservicio bajo demanda, amplio acceso la red, agrupación de recursos, rápida elasticidad y servicio medido; a continuación se enlistan dichas características y se hace una interpretación de las mismos en relación a las definiciones del NIST.

*a)* Autoservicio bajo demanda

Esta característica indica que cada cliente puede aprovisionarse de los servicios y de los recursos que requiera, según el tipo de tareas que necesite realizar en el servicio contratado en la nube, sin el requisito de que un humano intervenga en el proceso.

De tal suerte, los proveedores de servicios de cómputo en la nube solo deben poner en línea los distintos planes que ofertan a sus clientes, los clientes por su parte solo deben ingresar a la plataforma del proveedor y contratar el uso de los recursos que requieran. Por ejemplo, *software*, *hardware* o redes, en los cuales podrán montar los servicios que desean poner en línea.

*b)* Amplio acceso a la red

Esta característica hace referencia a la amplia variedad de dispositivos con los que se puede acceder a los servicios mediante la red de *Internet,* bajo estándares internacionales que permiten que los servicios en la nube sean accesibles desde cualquier lugar y mediante cualquier dispositivo capaz de conectarse a *Internet,* brindando con ello una ventaja operativa a los clientes de dichos servicios.

*c)* Agrupación de recursos

La agrupación de recursos se refiere a que los proveedores agrupan los recursos tecnológicos para servir a varios clientes con los mismos recursos, es decir, con un solo equipo servidor, mediante la virtualización de los servicios, pueden brindarse los servicios a varios clientes, según el servicio contratado. Estos equipos pueden estar agrupados aun cuando su ubicación sea distinta, pues la ubicuidad permite que bajo este modelo de servicio se pueda acceder a distintos servicios ubicados en locaciones distintas, como si se tratara de un servicio centralizado y exclusivo, aunque en realizad sea ubicuo y compartido.

*d)* Rápida elasticidad

Esta característica hace referencia a la facilidad con la que se pueden crecer los servicios acordados mediante contrato, pues a menudo, los clientes contratan solo los recursos informáticos que requieren al momento, pero debido a que estos requerimientos pueden variar de acuerdo a las necesidades de la empresa, los modelos de servicio de cómputo en la nube permiten que se incrementen o disminuyan fácilmente los recursos contratados.

*e)* Servicio medido

El servicio medido hace referencia al control y optimización automático de los sistemas de cómputo en la nube, utilizando mecanismos de medición según el tipo de servicio contratado, ya sea almacenamiento, procesamiento o infraestructura de red, permitiendo con ello dar un seguimiento del uso de los recursos, implementar controles y emitir notificaciones al usuario o al proveedor. Así se proporciona una mayor transparencia tanto al proveedor como al cliente de los servicios de la nube.

*B. Modelos de servicio de cómputo en la nube*

Dichos servicios se ofrecen en tres distintos tipos según las necesidades de la empresa, servicios que, aunque pueden ser combinados para satisfacer las necesidades del usuario final, se puede identificar claramente la diferencia de cada uno de ellos en infraestructura como servicio, plataforma como servicio y *software* como servicio (términos traducidos al español), mismos que se describen a continuación.

En una primera aproximación a los modelos de servicio de cómputo en la nube, según Luis Joyanes, se identifican como el modelo de despliegue y el modelo de servicio que constan de:

- Modelos de despliegue. Se refiere a la posición (localización) y administración (gestión) de la infraestructura de la nube (pública, privada, comunitario o híbrida).
- Modelos de servicio. Se refieren a los tipos específicos de servicio a los que se puede acceder en una plataforma *cloud computing* (*Software* como Servicio,

> Plataforma como Servicio e Infraestructura como Servicio)[32] [las cuales se describen a continuación].

Estos dos modelos que describe Joyanes Aguilar, representan el modelo de negocio tecnológico en el que los usuarios pueden contratar los recursos tecnológicos que requieran según sus necesidades, bajo las condiciones del tipo de nube que se contrate. A continuación, se describen los modelos de servicio y los modelos de despliegue.

*a.* Software como servicio

En los servicios de cómputo en la nube de software como servicio *(Software as a Service ó SaaS)*, encontramos una gran variedad de aplicaciones que se suministran bajo este modelo de servicio de computación en la nube. Por ejemplo, el más antiguo y que existía incluso antes de que se concibiera el paradigma del cómputo en la nube, es el correo electrónico, al cual se tiene acceso desde cualquier lugar y dispositivo.

Sin embargo, la característica de estas aplicaciones es la restricción que tiene el usuario para configurar los parámetros, cuando mucho tendrá algunas opciones de configuración de usuario, pero no de la aplicación en sí.

A este tipo de servicios se le une más recientemente los servicios de los sistemas de planificación de recursos empresariales, ERP por sus siglas en inglés de *(Enterprise Resource Planning)*, que permiten administrar los recursos de la cadena de suministro, seguimiento de clientes, recursos materiales, humanos y financieros mediante los módulos gestión de la cadena de suministro, SCM *(Supply Chain Management)*, gestión de la relación con el cliente, CRM *(Customer Relationship Management)*, planificación de requerimientos de materiales, MRP *(Material Requirements Planning)*, gestión de recursos humanos, MRH *(Human Resource Management)* y gestión de riesgos financieros, FRM *(Financial Risk Management)*, bajo un modelo de arquitectura orientada a servicios, SOA *(Service Oriented Architecture)*.

---

[32] Joyanes Aguilar, Luis, *Op. Cit*., p. 40.

Respecto a este tipo de servicio de nube Joyanes Aguilar menciona que “las aplicaciones son accesibles […] [desde] un navegador web […]. El usuario carece de cualquier control sobre la infraestructura o sobre las propias aplicaciones, excepción hecha de las posibles configuraciones de usuario”[33].

*b.* Plataforma como servicio

En este tipo de servicio se ofrecen plataformas como servicio *(Platform as a Service ó PaaS),* plataformas en las cuales las empresas puedan desarrollar sus propias aplicaciones y ponerlas en línea e incluso ofrecerlas como servicio a otros usuarios, sin tener que preocuparse de la infraestructura especializada que se requiere para que dichas aplicaciones funcionen.

Como ejemplo de ello podemos ver la gama de servicios que ofrece *Microsoft Azure*, en donde se pueden contratar servicios de entornos de desarrollo que tienen preinstaladas las aplicaciones necesarias para que los servidores ejecuten las aplicaciones web sin que el usuario cuente con los conocimientos avanzados sobre la administración de los servidores y las configuraciones del *software* que permite el despliegue de los contenidos web.

Es común que en este tipo de servicios se incluyan algunas aplicaciones dentro del mismo servicio; aplicaciones que permiten monitorear y administrar las aplicaciones que el usuario tiene en línea, esto con la intensión de poder obtener estadísticas que le permiten ir midiendo una serie de parámetros para perfeccionar los servicios.

Menciona Joyanes Aguilar que en este tipo de servicios “se le permite al usuario desplegar aplicaciones propias (ya sean adquiridas o desarrolladas por el propio usuario) […] de su proveedor, que es quien ofrece la plataforma de desarrollo y las herramientas de programación. [dejando al usuario la responsabilidad del] control de la aplicación, aunque no de toda la infraestructura”[34].

[33] *Idem.*
[34] *Idem.*

*c.* Infraestructura como servicio

La Infraestructura como servicio o *(Infrastructure as a Service ó IaaS)*, como se le conoce en el idioma español, corresponde a un servicio ofertado en la modalidad de nube, en el cual las empresas pueden contratar el uso de servidores, espacios de almacenamiento y redes de comunicación, en donde el usuario podrá instalar aplicaciones, generar discos virtuales o añadir discos virtuales adicionales, crear y administrar sus conexiones de red, así como administrar los usuarios y permisos. En otras palabras, lo que se usa y administra en este tipo de servicios es el *hardware* que el proveedor le renta al usuario para poner en la nube su información y/o aplicaciones.

Menciona Luis Joyanes, que en este tipo de servicios "el proveedor ofrece al usuario recursos como capacidad de procesamiento, de almacenamiento o comunicaciones que el usuario puede utilizar para ejecutar cualquier tipo de *software*, desde sistemas operativos hasta aplicaciones"[35].

*C. Modelos de despliegue de cómputo en la nube*

Los permisos que el usuario final tiene para administrar la tecnología que se contrata en modalidad de nube puede variar dependiendo del tipo de servicio contratado y del tipo de nube de que se trate. Entre los distintos tipos de nubes podemos destacar la nube pública, nube privada, nube comunitaria y nube híbrida, las cuales se describen a continuación.

*a.* Nube pública

La nube pública es un servicio que se encuentra disponible para el público en general, el cual puede ser gratuito o de paga según el tipo de servicio que se requiera. Entre los servicios más comunes podemos destacar el correo electrónico, el almacenamiento y las aplicaciones a las que se puede acceder desde cualquier dispositivo, utilizando solo un usuario y una contraseña.

Se denomina nube pública porque es un servicio disponible para todo el público, sin que el término signifique que los contenidos serán públicos; más bien se debe a

[35] *Ibidem,* p. 41.

que es de uso común y bajo las mismas características de acceso, destacando que los usuarios no cuentan con permisos para administrar la tecnología utilizada.

*b.* Nube privada

La nube privada corresponde a un modelo de servicio mediante el cual el usuario contratante tiene el control de la infraestructura contratada, permitiendo el desarrollo y/o el despliegue de aplicaciones en línea, con la característica de ser un servicio privado, es decir, solo la empresa contratante tiene acceso a esos recursos, por lo que los permisos para administrar dicha tecnología son más amplios que los que se tienen en los otros modelos de despliegue. De tal manera que el usuario contratante puede decidir a quién le permite el acceso a los contenidos.

Otra modalidad de nube privada es mediante la puesta en línea de aplicaciones y contenidos que residen en las instalaciones de la misma empresa propietaria de la tecnología y de las aplicaciones. Esto garantiza un control de acceso granular a los contenidos desde cualquier dispositivo que tenga *Internet* y sin la necesidad de contratar el servicio de un tercero.

*c.* Nube comunitaria

La nube comunitaria es un tipo de servicio en el que los contenidos a los que se puede tener acceso no solo pueden estar almacenados en los centros de datos de los proveedores de servicios de cómputo en la nube, sino que también se pueden compartir los contenidos de los usuarios mismos y que son accedidos por otras personas mediante servicios de nube híbrida.

Así en este tipo de despliegue se puede, a través de un servicio de nube desplegar información que se encuentra en distintas computadoras desde las cuales se puede dar el acceso para trabajo colaborativo, siendo el medio de acceso el servicio de la nube.

Otro ejemplo es el método utilizado para compartir contenidos punto a punto mediante el uso de una aplicación, la cual, al establecer una conexión a *Internet*, hace uso de un servicio de nube proporcionando el acceso a los contenidos que la comunidad de esa red ha puesto a disposición de la misma comunidad de la red.

*d.* Nube híbrida

El modelo de despliegue de nube híbrida integra características de los otros modelos de despliegue, ya que los contenidos, la tecnología utilizada y las aplicaciones disponibles en este modelo de despliegue pueden ser propiedad de la empresa que ostenta la titularidad de los contenidos o de un proveedor de servicios de cómputo en la nube.

La finalidad de esto es que se utilicen las tecnologías para dar soluciones más ágiles, utilizando el poder de cómputo de las grandes empresas tecnológicas, así como la gran variedad de aplicaciones y servicios disponibles, sin descuidar la seguridad de la información que no debe ser difundida por las implicaciones jurídicas o de impacto en las estrategias comerciales de la empresa.

Merceda esto, la información que se considere crítica o confidencial, permanece almacenada al interior de la empresa y con los permisos de acceso restringidos, mientras que las aplicaciones mediante las que se puede tener acceso a esa información pueden estar almacenadas en las instalaciones del proveedor de nube que permite la operabilidad del resto de la administración de la empresa.

Por consiguiente, en lo que respecta a la seguridad de la información, la nube representa una desventaja al ser un servicio proporcionado mediante el protocolo de *Internet* y por una empresa de reconocimiento internacional, la cual desde su concepción es conocida como una empresa que posee grandes cantidades de información.

Por otra parte, la información que se procesa y almacena mediante estos servicios, puede ser tratada por terceras empresas con las cuales el usuario no ha realizado contrato o convenio alguno, lo que representa un reto en cuanto a tratamiento de datos personales, llegando a derivar en violaciones al derecho a la protección de datos personales.

Por ello es que con los modelos de despliegue de nubes híbridas se busca mitigar el riesgo y, con ello, proteger los datos personales de la mejor manera posible, resguardándolos al interior de la empresa, permitiendo el acceso bajo demanda y

manteniendo el control de acceso en bitácoras que permitan la trazabilidad de la información.

Cabe señalar que cuando hablamos de tecnología de nube o cómputo en la nube, se hace referencia a la contratación de servicios en los que se utilizan equipos de cómputo y aplicaciones del proveedor y cuya ubicación física exacta puede ser desconocida. Sin embargo, se trata de *hardware* que es propiedad de una empresa.

En ese sentido, el término "nube" no existe, pues en realidad existe un espacio físico donde se almacena esa información y de la cual el contratante del servicio es el responsable legal según lo establece la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*[36].

### *1.4.2. Big Data*

Por su parte, el *Big Data* representa una ventaja para las empresas, ya que mediante esta tecnología es posible hacer recolección y análisis de grandes volúmenes de la información de todos y de nadie, es decir, de la información que se recupera mediante algoritmos de análisis de la actividad del usuario mientras navega en *Internet*, así como de información que se ha puesto en línea de manera intencional para la consulta en línea.

Podemos inferir que es un modelo de tecnología que se ha desarrollado para poder procesar grandes cantidades de datos que no es posible concentrar en un equipo de cómputo, por lo cual se ha optado por dejar la información en la red, y solamente mediante esta tecnología, analizarla para obtener conocimiento de ella y redirigir las acciones empresariales hacia la eficiencia y la eficacia de los recursos en beneficio de la empresa.

Pero, ¿qué es en realidad el *Big Data*? El *Big Data* "es el análisis de grandes volúmenes de información"[37]. Esta tecnología se divide en dos modelos: *Big Data Techonology*, que se encarga del estudio y desarrollo de las aplicaciones, así como de la configuración y mantenimiento de la arquitectura tecnológica de despliegue; y

---

[36] Publicada en el DOF el 5-julio-2010, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf. Consultado: 11/05/2018.
[37] González Díaz, Isaac, *Big Data para CEO's y Directivos de Marketing,* Kindle, 2017, p. 302.

*Big Data Analitycs*, que se ocupa de la explotación de los datos mediante técnicas de inteligencia artificial y lenguajes analíticos como *R* y *Phyton.*

Aunado al avance tecnológico y a las nuevas necesidades empresariales, se une la necesidad de "ser tratados de forma totalmente personalizada. Es por esto que, ser capaces de detectar sus gustos, se ha convertido en una necesidad de primer nivel para poder aumentar el volumen de ventas, dirigiéndolas de forma mucho más directa para lograr el éxito esperado"[38].

Existen estudios que infieren que los datos que se encuentran en la red se duplican cada dos años, por ello "los retos que debe gestionar el *Big Data* incluyen capturar, almacenar, buscar, compartir, transferir, analizar y visualizar"[39] grandes cantidades de información que se duplican a una velocidad impresionante.

Ante esta gran cantidad de datos, las empresas requieren tener un conocimiento más concreto, no solo de lo que sucede en la actualidad sino de lo que sucederá en el futuro. Sin embargo, el *Big Data* no es solo el análisis de los grandes volúmenes de información, "sino que éste es sólo una parte del rompecabezas, siendo muy diversos los parámetros que se tienen en cuenta en cada ocasión"[40].

Así mismo, mediante esta tecnología, es posible analizar incluso las redes de contactos de los clientes, convirtiéndose en una herramienta para la localización de clientes potenciales, a los cuales se les puede hacer llegar de manera discreta publicidad de artículos que pueden ser de su interés, aumentando las posibilidades de venta.

Jorge Mendes explica la gran cantidad de datos de las 7 Vs que son el "Volumen, la variedad, el valor, la visualización, la variabilidad y la veracidad"[41], de los cuales se hace una síntesis en los próximos párrafos para dejar en claro a que se refiere cada uno de estos términos, los cuales en la actualidad son de gran relevancia, no

---

[38] PowerData, ***Del bit… al Big Data,*** s.a., p. 5, http://cdn2.hubspot.net/hub/239039/file-359994269-pdf/docs/PowerData_-_Del_bit%E2%80%A6_Al_Big_Data.pdf. Consultado: 01/06/2018.

[39] Sevillano Pérez, Felipe, "Big Data", *Economía industrial,* (Ejemplar dedicado a: Ciudades inteligentes), núm. 395, 2015, p. 75, https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/395/F%20SEVILLANO%20PEREZ.pdf. Consultado: 01/06/2018.

[40] PowerData, O*p. Cit.,* p. 3.

[41] *Cfr.* Mendes, Jorge, *Big Data La primera guía completamente en español explica Big Data y sus aplicaciones,* Kindle, 2018.

solo para las empresas, sino también para la sociedad en general como usuarios activos de la tecnología.

Así pues, el *volumen* de datos digitales que se generan en la actualidad se expande a una velocidad impresionante gracias a la tecnología del *IoT*, que permite recolectar información de cualquier dispositivo capaz de conectarse a *Internet* y ya no solo de las computadoras, esto provoca que cada dos años se duplique la información actual y aumente la velocidad de expansión en los próximos años.

La *variedad* de los datos se refiere a que el *Big Data* se alimenta de una gran variedad de presentación de datos, los cuales están ordenados en archivos y bases de datos de manera no estructurada pero que son legibles mediante aplicaciones de procesamiento como *Hadoop, MapReduce, Hive,* entre otras.

La *velocidad* se refiere a la velocidad con la que son generados los datos, almacenados y analizados, a diferencia de la generación de archivos por lotes que tardaban tiempo en ser procesados por las computadoras, con la tecnología de *Big Data*, esto se puede hacer en tiempo real gracias a la velocidad de *Internet* y a la capacidad de los dispositivos para comunicarse mediante el protocolo de *Internet*.

Esto hace posible que tan solo en un lapso de un minuto, se envíen 200 millones de correos, se suben 100 horas de video a *YouTube*, son vistas 20 millones de imágenes, son enviados 300,000 tweets y se realizan 2.5 millones de búsquedas en Google[42].

El *valor* de los datos no se refiere en sí al valor de la información, sino al valor que puede cobrar al ser analizado por las empresas para convertir esa información en el conocimiento que le permita guiar su actividad comercial con mayor eficiencia y mayores posibilidades de venta, que se traducen en el valor de la información del *Big Data.*

La *visualización* hace referencia a las herramientas que se utilizan para hacer el análisis de la información, lo que se mencionó anteriormente como *Big Data Analitycs,* que permite tomar ese mundo de información para sintetizarlo y obtener resultados visiblemente concretos, claros y útiles para la empresa. A esta tarea de transformar en útiles los datos, también se le conoce como ciencia de datos.

---

[42] *Cfr.* Jorge Mendes, *Op. Cit.*

La *variabilidad*, la información puede tener una variedad de significados y puede ser presentada de distintas maneras, a esto se le conoce como variabilidad de la información, por lo que los algoritmos de *Big Data* deberán incorporar la inteligencia artificial necesaria para poder contextualizar la información de acuerdo al tema para el que se requiere procesar la información.

La *veracidad* de la información cobra importancia no solo para el derecho a la información, sino que también influye en las decisiones de los directivos de las empresas cuando la información que se analiza es defectuosa, ya que los resultados de dicho análisis pueden poner en riesgo la operación de la empresa. Por ello, mediante esta tecnología e inteligencia artificial se debe buscar solo la información que es confiable, es decir se debe analizar solo la información que es verdadera para el tema en cuestión y descartar la información considerada como basura.

Si bien es cierto que esta actividad es una ventaja competitiva para la empresa, también representa un riesgo legal, ya que la línea entre lo legal e ilegal del tratamiento de los datos personales es muy delgada, pudiendo mediante esta tecnología, vulnerar la intimidad de las personas y violentando su derecho a la protección de datos personales e incluso la misma integridad física de las personas en caso de ser vulnerados por los delincuentes informáticos.

### *1.4.3. Inteligencia Artificial*

El término de inteligencia artificial fue acuñado en el año 1960 por McCarthy “para denotar los métodos algorítmicos que hacían pensar a los ordenadores”[43]. Durante los años setenta surgen los denominados sistemas expertos que son capaces de codificar el conocimiento con base en decisiones algorítmicas que dan origen a la toma de decisiones por los sistemas basados en conocimientos humanos.

El método utilizado por los sistemas expertos pronto se vio superado por los problemas que se planteaban en el mundo real, pues ya no era suficiente que los sistemas basaran sus decisiones en los métodos decisionales del *“si…entonces”*,

[43] Aguilera García, Edgar Ramón, *Inteligencia Artificial Aplicada al Derecho,* México, Universidad Nacional Autónoma de México, 2007, pp. 36-37.

sino que se presenta la necesidad de llevar a los sistemas más allá, desarrollando algoritmos que permitieran a los sistemas aprender para generar nuevos conocimientos basados en la información suministrada como materia prima.

A este tipo de métodos de análisis de información también se les conoce como redes neuronales. Estos sistemas buscan reproducir el modelo del cerebro humano en los sistemas informáticos para que puedan ser capaces de aprender y generar nuevos conocimientos de manera autómata.

Un término quizá más reciente es el de aprendizaje máquina por su traducción al español del término *"Machine Learning",* que es un método utilizado en los algoritmos de inteligencia artificial, que pueden ser entrenados mediante la introducción de muestras *"inputs"* a partir de las cuales los sistemas pueden aprender a desarrollar un nuevo conocimiento para aprender a dar respuestas automáticas sin la intervención humana y con un elevado grado de precisión.

Finalmente, como sea que se les llama a estos algoritmos de programación (sistemas expertos, redes neuronales o *machine learning*), se sintetizan en la rama de las tecnologías de la inteligencia artificial que buscan reproducir el funcionamiento del cerebro humano en las computadoras. Todas ellas están basadas en el análisis de la información recolectada, de la cual derivan nuevos conocimientos de manera automática sin la intervención humana; adquiriendo conocimiento de las mismas acciones históricas para perfeccionar su funcionamiento y precisión en los resultados.

Esta tecnología está siendo implementada en varias áreas del conocimiento en las que se busca reducir los esfuerzos humanos, aumentar la productividad y mejorar los procesos para la toma de decisiones, convirtiéndose en una herramienta indispensable para las empresas que buscan ser competitivas en la economía de la información.

Un ejemplo claro de estas tecnologías son los algoritmos de Google que pueden analizar los gustos de las personas mediante su historial de búsquedas en *Internet*; pueden generar perfiles digitales de las personas para conocerlas mejor y para poder ofrecer los productos de acuerdo a su perfil. Esto se logra mediante algoritmos que incorporan inteligencia artificial para aprender sobre la persona que

usa cierta computadora de la cual se tiene una huella digital que identifica inequívocamente a las personas, aun y cuando no tengan una cuenta de correo de Google.

También los algoritmos de Google incorporan semántica web que se combina con la inteligencia artificial, haciendo que el usuario tenga una mejor experiencia en la navegación por *Internet* al usar el motor de búsqueda de Google, ya que aprende sobre la persona y comienza a entregar resultados de los intereses personales al momento de realizar búsquedas en *Internet*. Esta tecnología beneficia a las empresas debido a la eficiencia de las campañas publicitarias que se contratan mediante servicios publicitarios de Google, por poner un ejemplo.

Incluso son tecnologías que se están implementando en las áreas jurídicas para los procesos de impartición de justicia, en donde mediante sistemas de inteligencia artificial se analizan los casos y se aplica una sentencia basada en el conocimiento de la información que se presenta como pruebas del caso, con la ventaja de no involucrar sentimientos humanos en la decisión de la sentencia.

Esto presenta un gran avance de la tecnología en beneficio de la sociedad y ya no solo para las empresas, pues al tener un sistema de impartición de justicia imparcial, se puede decir que mediante la aplicación de la tecnología es posible combatir la corrupción en los procesos judiciales. Sin embargo, sigue siendo un punto de preocupación dejar la decisión en manos de una tecnología creada por el hombre y que se desconoce de cierta manera el nivel de aprendizaje y las variaciones generadas por las orientaciones automáticas del sistema.

Esta tecnología puede ser desplegada en sistemas locales o en sistemas de nube, según las necesidades de la empresa y la finalidad de la aplicación de inteligencia artificial. El modelo de despliegue dependerá de la finalidad buscada por la empresa sin que esto interfiera en los resultados específicos para los que haya sido creada la aplicación.

En todo caso, la inteligencia artificial busca orientar el conocimiento derivado de la recolección de información mediante técnicas de *Big Data* y dar a conocer los resultados mediante aplicaciones que pueden estar alojadas en servicios de nube o al interior de las empresas, permitiendo que las acciones directivas tengan un

conocimiento más afinado en el menor tiempo posible con el menor esfuerzo humano posible.

Sin embargo, el fenómeno de las tecnologías de la información y comunicación, aunado a la evolución social que ha ido distorsionando la aplicación de la tecnología para diversos fines distintos a los planteados en los inicios del desarrollo tecnológico, ha creado la necesidad de legislar en la materia para dar orden y garantizar el respeto a los derechos humanos y al desarrollo económico de las naciones mediante ordenamientos jurídicos que regulan la actuación de la sociedad y la aplicación de la tecnología para fines benéficos y actos lícitos.

### *1.5. Hacia una definición de Información*

Ya se ha dicho que las empresas requieren recolectar y analizar información para obtener conocimientos que le permitan guiar sus acciones futuras, adecuar sus estrategias de mercado y optimizar sus recursos. Esto se da como acción de un proceso de comunicación, en donde se supone debe existir un emisor que proporciona la información a la empresa receptora, para que ésta, a su vez, pueda someterla a un análisis que, de acuerdo a las necesidades, derive en un nuevo producto informativo útil para la toma de decisiones.

Más adelante se hablará del Derecho de la Información como una ciencia jurídica que ha sido creada para regular la actividad de recolección y explotación de la información; de igual manera se hablará del derecho a la información, un derecho que permite a las personas (físicas o morales), investigar, recibir y difundir información por cualquier medio de expresión y comunicación, así como el derecho a la protección de datos personales, que busca la protección de la vida privada de las personas al relacionarse con sus iguales y con las empresas comerciales que hacen uso de sus datos para la adquisición de productos y servicios.

Los anterior, en relación con lo que ya se ha dicho sobre la sociedad de la información, muestra la inevitable relación entre la sociedad, el derecho, la tecnología y las empresas; elementos necesarios para el desarrollo de una sociedad libre, responsable, con derechos y obligaciones, con amplias posibilidades para contribuir al desarrollo económico.

Se entiende, entonces, que los derechos mencionados buscan regular las conductas humanas en el disfrute de las ventajas que la tecnología ofrece en todos sus ámbitos, pero dentro de un marco normativo que busca la protección de los derechos de los seres humanos. De acuerdo a los derechos mencionados, todo ello, en torno a la información con la que las personas interactúan día con día.

De tal manera que, parece necesario para este tema analizar de manera más profunda qué es la información, con la intención de acercarnos a una definición de la misma. Para ello, nos remitimos a los orígenes de la comunicación, entendiendo a ésta como una condición necesaria para la evolución de la humanidad, pues de la comunicación se genera información; elemento indispensable para la producción del conocimiento que permite el desarrollo económico de las naciones, así como factor determinante para la evolución de la sociedad.

Sin embargo, se desconoce a ciencia cierta cuándo fue la primera vez que el ser humano pronunció la primera palabra, tampoco se tiene una fecha exacta que nos refiera a partir de cuándo es que los seres humanos comenzaron a comunicarse entre sí. No obstante, retomando los indicios de la prehistoria, es posible advertir que desde los inicios de la humanidad se comenzó a desarrollar un código de comunicación, que en principio se cree, era con base en señas, gestos y signos.

Posteriormente, como efecto de la misma evolución de la humanidad, el lenguaje se transformó en palabras que comenzaron a tomar significados, entendidos por las comunidades en donde se desarrollaba ese lenguaje, convirtiéndose así, en un nuevo código de comunicación mediante el cual se transmitía el mensaje que el emisor quería dar a conocer al receptor, y el cual podía ser interpretado solo por aquellas personas que conocieran el código de comunicación utilizado.

Así, desde los inicios de la humanidad, la comunicación ha venido evolucionando sin tener los indicios concretos que den pauta para poder retomar una fecha exacta como referencia, incluso se habla de diversos tipos de escritura. Sin embargo, Sumeria y Egipto poseen buena parte de los indicios del inicio de la escritura analítica[44].

[44] *Cfr.* Ruíz García, Jesús; Baño Gimeno, M.A. Pilar y Secadas Marcos, Francisco, “Evolución Histórica de la Escritura” *Estudios*, Madrid, España, 1985, pp. 196-207.

Han sido diversos los hallazgos en torno a los indicios del inicio de la escritura, como diversos han sido los medios en donde se plasmaba la escritura, pasando de las tablillas usadas por los sumerios, a los rollos de papiro usados por los egipcios en los años 2500 a.C., la caída del imperio romano que generó la necesidad de la creación de un alfabeto fonético, hasta llegar al surgimiento de la imprenta de Gutenberg[45].

Consecuentemente, el desarrollo de la humanidad ha dado origen también a la evolución de la escritura como medio de comunicación de pensamientos e ideas, hasta llegar a la comunicación como la conocemos hoy en día, y que sigue evolucionando en su forma de trasmitirse, mediante diversos canales que hacen posible que las personas puedan comunicar y recibir información sin limitación de fronteras de lugar y tiempo, conformando así, dos de los elementos indispensables del derecho a la información.

En todo caso, la comunicación genera información, ésta se obtiene o proporciona en diversas presentaciones, lo que produce cambios en la manera de ser tratada, dependiendo si se trata de información sonora, gráfica, sensitiva o literaria, pues no se procesa de la misma manera un sonido que un texto impreso, por ello, si se quiere obtener conocimiento de la información, es necesario tratarla de manera distinta según el medio por el cual se haya obtenido para lograr el objetivo perseguido.

Así entonces, a partir de la escritura se hace posible tener la información disponible para su consulta y análisis; susceptible de ser procesada de distintas maneras para interpretar y generar nuevas informaciones (conocimiento) a partir de ella, dando como resultado un nuevo producto informativo derivado de la transformación de la información.

Esta evolución responde a la necesidad de la ya mencionada sociedad de la información, que le ha dado un nuevo sentido de utilidad a la comunicación de sentimientos, opiniones, ideas y gustos de las personas, que han sido tomadas para distintas finalidades. Así, el lenguaje se convierte en nuevos códigos de comunicación, representados en tecnologías autónomas, capaces de interpretar la

[45] *Cfr.* Carr, Nicholas, *Superficiales,* Taurus, México, D.F., 2015, pp. 78-93.

actividad de las personas para obtener más información de la que se puede conocer mediante el proceso de comunicación, en el que se supone existe un emisor, un código, un mensaje y un receptor.

Actualmente se puede aseverar que la sociedad depende de la información, para sobrevivir y desarrollarse en la selva de la competitividad que representa el cambiante mercado tecnológico, al grado que las nuevas generaciones no pueden imaginar un mundo sin la tecnología, que de cierta manera resulta invasiva pero necesaria para la sociedad que se ha vuelto dependiente de los dispositivos electrónicos y del *Internet*.

Al integrar las tecnologías de la información y comunicación en los procesos de comunicación entre personas, se genera una gran cantidad de información, susceptible de ser transmitida por canales tecnológicos y en lenguaje binario, código interpretado solo por las computadoras como su lenguaje natural, pero representado en lenguaje natural como código común para los destinatarios.

De tal manera que las tecnologías de la información y comunicación han transformado la información en un concepto cada vez más ubicuo, lo mismo ha sucedido con las diversas tecnologías que permiten su procesamiento y con la sociedad que ha de interpretarla, con la cultura e incluso con otras ciencias. Así como "[…] la irrupción de la teoría de la información y el desarrollo tecno-científico que la ha acompañado han impactado de múltiples modos a la sociedad"[46].

Como ya se ha mencionado, la sociedad actual depende de la información, pero, ¿Qué es en realidad la información que se ha vuelto tan indispensable para el desarrollo de las naciones en todos los ámbitos?, incluso, la información se ha convertido en algo tan delicado que puede poner en riesgo la estabilidad social, económica o la seguridad mundial.

Diversos autores son los que han tratado de definir el término *información,* sin embargo, la han tratado desde distintas corrientes, dando un significado acorde a la ciencia en la que se desarrolla el concepto sin poder definir claramente de manera universal dicha noción. No obstante, algunas de las aproximaciones son:

---

[46] Ríos Ortega, Jaime, "El concepto de información: dimensiones bibliotecológica, sociológica y cognoscitiva", *Investigación Bibliotecológica,* Vol. 28, Núm. 62, enero/abril 2014, pp. 144-145.

> […] la información en la teoría de la comunicación tiende a verse como un valor inicial alterado por los procesos de ruido y entropía que afectan a la señal que la transmite. En la teoría del procesamiento de la información, ésta es vista como una entidad percibida, seleccionada, almacenada y comunicada por los organismos de cara a su supervivencia y realización. En la teoría de la gestión de la información, la información es vista como un recurso valioso susceptible de gestión económica. […][47]

Otra definición de información la encontramos en la tesis de licenciatura de Martha Cristina Jiménez Rosano, en donde menciona que "la información es un conjunto de mecanismos que permiten al individuo retomar los datos de su ambiente y estructurarlos de manera determinada, de modo que le sirvan como guía de su acción. No es lo mismo que comunicación, aunque la supone"[48]. De tal manera que la información es el elemento susceptible de ser comunicado u obtenido, mediante un proceso de comunicación y que transmite conocimientos que se plasman a manera de información, capaz de generar nuevos conocimientos.

Idalberto Chiavenato, reconocido autor en las ciencias administrativas, define a la información como:

> Conjunto de datos con un significado, o sea, que reduce la incertidumbre o que aumenta el conocimiento de algo. En verdad, la información es un mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones[49].

Como se puede observar, las definiciones pueden ser diversas dependiendo del área de estudio en la que se desarrolle la investigación. No obstante, retomando lo que refiere la Real Academia de la Lengua Española, se menciona que la información es la "comunicación o adquisición de conocimientos que permiten

---

[47] García Marco, Francisco Javier, "El Concepto de Información: Una aproximación transdisciplinar", *Revista General de Información y Documentación,* Vol. 8, Núm. 1., Madrid, Servicio de Publicaciones Universidad Complutense, 1998, p. 307.

[48] Jiménez Rosano, Martha Cristina, *El ensayo fotográfico como Diseño de Información. El uso de la fotografía en la investigación exploratoria de un fenómeno social*, Puebla, Universidad de las Américas Puebla, 2005, p. 13, http://catarina.udlap.mx/u_dl_a/tales/documentos/ldf/jimenez_r_mc/. Consultado: 21/06/2018.

[49] Chiavenato, Idalberto, *Introducción a la Teoría General de la Administración*, 7a ed., México, McGraw-Hill Interamericana, 2006, p. 110.

ampliar o precisar los que se poseen sobre una materia determinada”[50]. Esta definición supone un conocimiento previo del que deriva la información; dicho conocimiento se traduce en el cúmulo de los datos susceptibles de ser comunicados o adquiridos, dando como resultado información de la cual se genera conocimiento específico, necesario para la toma de decisiones personales o empresariales en situaciones concretas.

De esta manera, se puede definir la *información como un conjunto de datos que pueden ser adquiridos o proporcionados mediante cualquier medio de comunicación y en cualquiera de sus posibles representaciones, (audibles, visibles o sensitivos), susceptibles de ser procesados y transformados para generar nuevos conocimientos que orienten las futuras acciones humanas en la toma de decisiones, aumentando el grado de certidumbre de los resultados perseguidos.*

La información se puede representar en sonidos o imágenes que pueden ser procesados por el cerebro humano; por símbolos o códigos que pueden ser procesados por los dispositivos tecnológicos. En cualquiera de los casos, al ser procesada esa información, debe convertirse en la materia prima de los conocimientos que regulan las acciones humanas en busca de un mejor futuro.

De modo que podemos decir que aquellos datos que generan información que no proporciona ningún conocimiento de utilidad para la sociedad, pierde su significado de información, quedando en el plano de los datos que no son capaces de guiar las acciones humanas hacia un futuro más cierto, por no generar nuevos conocimientos.

De esta manera, la misma definición de información nos aproxima al derecho a la información, que regula la circulación de la información y dota de facultades a las personas para poder investigar, recibir y difundir información *veraz* y de interés social, proporcionando a la sociedad de la información los elementos necesarios que les da la capacidad de tomar decisiones en beneficio de la comunidad, en un intento por mejorar la calidad de vida de las personas.

---

[50] Real Academia de la Lengua Española, *Información*, [En línea], 2019, http://dle.rae.es/?id=LXrOqrN.

*1.6. Reflexiones finales*

Es evidente que el desarrollo tecnológico no se detendrá para esperar a que la sociedad, el derecho y la tecnología caminen a la par, sino por el contrario, la tecnología nos obliga a caminar a marchas forzadas para tratar de adoptar las nuevas tecnologías a nuestro actuar cotidiano, sea para uso personal o empresarial.

Concretamente hablando del sector empresarial, las empresas se ven obligadas a incorporar las tecnologías de la información y comunicación a sus procesos de negocio, adoptando tecnologías para la recolección, análisis y tratamiento de datos, que en principio pareciera que no son personales, pero que indudablemente el análisis de dichos datos puede llevar a la identificación de las personas mediante la huella digital que muestra sus gustos, pensamientos, afiliaciones políticas y religiosas, patrones de conducta en la red, entre otros.

Visto desde esa perspectiva, todo aquello que se recolecta en la red mediante distintas tecnologías, cae en el terreno de los datos personales, pues al final es información que obtiene de las personas que navegan en *Internet*, sea de manera silenciosa –pasiva– o de manera activa, es decir, pidiendo al usuario que teclee sus datos para poder recibir algún producto o servicio.

Sin importar cuál es el método de obtención de los datos, la aplicación de tecnologías de análisis y predicción aportan a las empresas que usan estas tecnologías una ventaja competitiva, la cual es necesaria en esta economía digital en la que toda ventaja de mercado depende de un buen análisis de la información con que se cuenta para orientar las acciones futuras.

Así entonces, es necesario aceptar la necesidad de hacer uso de la tecnología existente e incluso trabajar para desarrollar nuevas tecnologías que aporten ventajas en el mercado, pero también es necesario conocer sobre los derechos humanos, ya que el uso de la tecnología a menudo se relaciona con la violación de los mismos. Es de entender que esto suceda, pues como ya se dijo anteriormente, las leyes no caminan a la par del desarrollo tecnológico.

Sin embargo, al momento de hacer uso de la tecnología y a la luz del derecho a la protección de datos personales, es necesario proporcionar al titular de los datos toda la información que le permita conocer el tratamiento de los mismos, para que

éste decida de manera informada, de acuerdo a sus intereses y necesidades, si proporciona su información bajo las condiciones que le han sido dadas a conocer mediante el aviso de privacidad.

Es importante recordar que la misma Ley menciona que es ilícita la recolección de información a través de medios engañosos; en este supuesto puede encajarse la recolección pasiva de datos, es decir sin que el usuario se entere. Por ello además de tener en cuenta lo que establece la Ley, es necesario fomentar los valores éticos y morales como principios rectores de una sana convivencia social y el respeto de los derechos humanos.

Solo de esta manera podremos hacer uso de la tecnología para disfrutar de sus bondades en el desarrollo empresarial o personal; sea por necesidad, por gusto o con el objetivo de mejorar la calidad de vida, pero con apego a la normativa nacional e internacional, que impida que se menoscaben los derechos de las personas a cambio de una remuneración económica.

En retrospectiva, es de observar que el uso de la nube como entorno tecnológico de tratamiento de datos personales, supone la transferencia –término que se abordará con más detalle en el tercer capítulo– de los datos personales a un tercero e incluso fuera del territorio nacional, lo que conlleva la obligación de dar a conocer al titular sobre dicha transferencia y a solicitar su consentimiento, cosa que, al momento, muchas empresas no están haciendo al usar esta tecnología para el tratamiento de los datos personales.

Esto supone la violación de un derecho humano a consecuencia del desconocimiento de la Ley. Sin embargo, no significa que la tecnología sea violatoria de derechos humanos por su naturaleza, sino, más bien, la ubicuidad de la misma y su potencial ilimitado aún no explorado, no ha permitido el desarrollo de la legislación al grado de contemplar todos los supuestos necesarios para armonizar la tecnología con las leyes en pro de los derechos humanos, sin tener que limitar el uso de la tecnología, permitiendo así el desarrollo empresarial y económico, mediante el uso de la misma y en beneficio de la sociedad.

*Cambia tus pensamientos y*
*cambiarás tu mundo*

*- Norman Vincent Peale -*

# CAPÍTULO SEGUNDO

## NATURALEZA JURÍDICA DEL DERECHO A LA INFORMACIÓN

### *2.1. Definición de Derecho de la Información*

A manera de introducción al tema, pero sin intensión de profundizar en ello, resulta importante remontarnos a la transición entre la Revolución Industrial y la actual sociedad de la información, etapa que se desarrolló entre los años 1760 a 1870, la cual se caracterizó por ser un periodo de grandes cambios sociales, económicos, culturales y de avances tecnológicos, que dieron origen a los cimientos de la llamada sociedad de la información que se ha venido gestando desde los años 70s, pasando por varias etapas de adaptación a consecuencia del desarrollo de las nuevas tecnologías de la información, elemento fundamental de esta sociedad.

En esa transición, se impulsó el desarrollo de nuevas tecnologías para la automatización de procesos productivos en las empresas. No debemos omitir también que en este periodo aconteció la Segunda Guerra Mundial, que también tuvo gran influencia en el descubrimiento de nuevas tecnologías para usos militares[51], tanto para el desarrollo de armas avanzadas, como para agilizar la comunicación y dificultar la intercepción de los mensajes de los contrarios.

Sin embargo, la aplicación de dichas tecnologías no terminaba ahí, pues, aunque en un principio su aplicación fue industrial, la Segunda Guerra Mundial fue un factor de desarrollo tecnológico, tecnologías que posteriormente fueron adoptadas para nuevas aplicaciones en el sector comercial. Esto dio como resultado la creación de las primeras computadoras de propósito general, entendidas en un principio como máquinas electrónicas capaces de procesar grandes cantidades de información a alta velocidad, superando por mucho las capacidades humanas.

---

[51] *Cfr.* Peirano, Martha, *El enemigo conoce el sistema,* Penguin Random House Grupo Editorial, Barcelona, 2019, pp. 90–93.

Dicho desarrollo tecnológico fue transformando el paradigma de la comunicación, desembocando en una transformación social que trajo consigo grandes cambios en la conducta de las personas, así como en la manera de comunicarse; lo anterior hizo necesario el reconocimiento de nuevos derechos, obligaciones y sanciones derivadas del uso de las nuevas tecnologías, propias de la sociedad de la información.

La concepción de esta nueva etapa supone un cambio de paradigma social, pues con el uso de las tecnologías se comienza a transitar hacia una sociedad que basa sus esfuerzos y enfoca sus recursos para el procesamiento de la información, de la cual se obtiene el conocimiento necesario para enfocar los esfuerzos empresariales hacia objetivos concretos en el mercado, donde se desarrolla la economía global. Sin embargo, esto hace necesaria la existencia de una regulación creada para la información, a lo que Desantes le llamó el Derecho de la Información.

Así entonces, la comunicación ha evolucionado de manera tan vertiginosa que los códigos mediante los cuales se comunica la sociedad, cambian tanto en forma como en método, dando como resultado la necesidad de crear nuevos canales de comunicación que, a su vez, han evolucionado de tal manera que los mensajes susceptibles de codificar y transmitir, son tan diversos que se vuelve necesario regular la comunicación mediante la creación de normas jurídicas, en busca de una sana convivencia social. Eso tiende a permitir el hacer uso de los nuevos descubrimientos comunicativos sin que estos tengan por objeto o fin, la afectación de alguna esfera de la personalidad.

Respecto a este derecho menciona Desantes que, es la información lo que interesa en primer término; que en un amplio sentido la información supone un estudio pluridisciplinar, de aquí que se desprende el derecho bajo el aspecto informativo o que podríamos entender como Derecho de la Información, teniendo como principal objeto el derecho de estar informado y de tener derechos sobre la información que como personas estemos generando, sea personal, literaria, de obras inéditas o de cualquier otra índole[52].

[52] *Cfr.* Desantes, José María, *Fundamentos del Derecho de la Información,* Confederación Española de Cajas de Ahorros, Madrid, 1977, p. 34

Asimismo, Desantes define el derecho de la Información como "[…] la Ciencia jurídica universal y general que, acotando los fenómenos informativos, les confiere una específica perspectiva jurídica capaz de ordenar la actividad informativa, las situaciones y relaciones jurídico-informativas y sus diversos elementos, al servicio del derecho a la información"[53].

Consecuentemente, el derecho de la información retoma la evolución causada como efecto de la Segunda Guerra Mundial para dar paso a la sociedad de la información, y a partir de ello analiza la conducta de las personas, derivando así en una ciencia jurídica para la regulación del fenómeno informativo, concluyendo según Desantes en una ciencia jurídica que:

> Estudia el ordenamiento informativo y, a partir de su valoración, juzga si es aceptable o no y facilita principios para su correcta regulación. El sustantivo Derecho significa aquí Derecho objetivo; y el sustantivo Información, un concepto institucional de esta palabra que engloba a todos los elementos del proceso informativo. Por supuesto, no hay que confundirlo con el "derecho a la información", con minúsculas, como derecho subjetivo, fundamental con arreglo a los términos de nuestra Constitución; humano conforme a la Declaración de la ONU de 1948; e innato según la tradición jurídica occidental […]. Aquí el sustantivo Información se concreta a un mensaje determinado: derecho a la información equivale así a derecho al mensaje[54].

De esta definición podemos inferir entonces que el Derecho de la Información es más que un derecho, una ciencia y, por ende, más amplio que el derecho a la información, al tratarse de un derecho que se ha creado por y para la información. Por supuesto que está relacionado el uno con el otro, pero, mientras que el derecho a la información se concreta en un entramado jurídico que tiene como objeto el mensaje informativo y en las facultades que tienen las personas – el sujeto – para ejercer dicho derecho, el Derecho de la información es una ciencia, en la cual se ha englobado todo el conjunto de normas jurídicas que regulan el uso de la información, el ejercicio de las facultades de las personas y al Estado, para que exista la circulación de información veraz, de manera libre y sin censura y con la garantía de respeto a los derechos humanos.

---

[53] *Ibidem, p. 244*

[54] Desantes, José María, *Derecho a la información. Materiales para un sistema de la comunicación,* Fundación COSO, España, 2004, p. 69.

De tal manera que el derecho de la información según Ernesto Villanueva, es "la rama del derecho público que tiene por objeto el estudio de las normas jurídicas que regulan, *lato sensu*, las relaciones entre Estado, medios y sociedad, así como, *strictu sensu,* los alcances y los límites del ejercicio de las libertades de expresión y de información y el derecho a la información […]"[55].

Así entonces, el ejercicio de las libertades de expresión y las facultades del derecho a la información, son facultades ejercidas por los sujetos del derecho de la información, mismos que define Desantes como *sujeto universal, sujeto cualificado y sujeto organizado*. Entendiendo al sujeto universal como todas las personas, al sujeto cualificado como aquella persona que desempeña una función de informador (periodistas) y al sujeto organizado como todas las empresas informativas que difunden información de interés social (medios de comunicación).

Cabe señalar que en toda sociedad es necesario el ejercicio de las libertades de expresión para que exista una comunicación, lo que viene a conjuntar la idea de "la doctrina científica informativa [que] ha refrendado que comunidad y comunicación son ideas que se relacionan entre sí: No hay comunidad sin comunicación, no hay comunicación sin comunidad"[56].

Por consiguiente, la comunicación se da para el desarrollo social y económico de la comunidad, al perseguir este objetivo deben tratar con información y con personas, lo que hace que esta ciencia jurídica sea compleja, ya que el fenómeno informativo en su modelo actual, propio de la sociedad de la información, requiere no solo la búsqueda de la verdad, sino también la aplicación de normas que garanticen la convivencia respetuosa entre la sociedad, incluyendo la conducta de las personas en los entornos tecnológicos.

Consecuentemente, el derecho de la información tiene por objeto proteger el derecho a la información; este nuevo derecho viene determinado por la información, buscando conocer la verdad del porqué de las cosas que suceden en la comunidad, es decir, va más allá de la simple observación en un intento por lograr obtener un

---

[55] Villanueva, Ernesto, *Derecho de la Información*, México, Miguel Ángel Porrúa, 2006, p. 10

[56] Aguirre Nieto, Marisa, "El Derecho de la Información como Ciencia", en Bel Mallen, Ignacio y Corredoira y Alfonso, Loreto, (ccord.), *Derecho de la Información,* España, Editorial Ariel, S.A., 2003, p. 54.

conocimiento científico partiendo de la información; como se hace en las empresas para poder conocer la verdad sobre el mercado global para aumentar sus acciones comerciales en un marco de regulación jurídica.

Así, al existir la necesidad de comunicación entre las personas de una comunidad, esa comunidad evolucionó en torno a los fenómenos y a los nuevos conocimientos de las personas; por ende, el derecho de la información no crea los fenómenos, sino que los reconoce y los acoge en las normas jurídicas para regularlos, logrando así el objetivo del derecho que busca regular la convivencia entre las personas y el entorno que nos rodea.

Como se mencionará en lo subsecuente, las empresas son un ente comercial formado por varias personas que unen esfuerzos y recursos para desarrollar alguna actividad económica; dichas empresas para poder operar requieren de información veraz que orienten sus estrategias de mercado. Consecuentemente, podemos aseverar que “la información no es un lujo sino la exigencia de saber que pasa en el mundo”[57] para poder tomar decisiones con base en conocimiento de lo que está aconteciendo en el mundo real.

Esos acontecimientos se pueden recolectar mediante tecnologías de la información y comunicación y algoritmos de inteligencia artificial, que pueden estar alojados en la nube; lo que por sí mismo ya es un reto para las empresas, que además deben orientar sus acciones bajo la regulación que supone el derecho de la información para obtener el beneficio de las tecnologías en el proceso de recolección, procesamiento y divulgación de la información. Dichos beneficios se concretan al obtener de la información el conocimiento, y del Derecho de la Información la certeza de que la información que se obtiene es veraz y de utilidad para la toma de decisiones.

Por ello, “es interesante detenerse a observar la historia de ese proceso que camina marcado por las exigencias del desarrollo tecnológico y por los requerimientos exigidos por la sociedad hasta llegar a la idea de conceptuar a la

[57] *Ibidem,* p. 47.

información como un saber que debía ser tratado científicamente”[58], del cual nos ocuparemos más adelante.

Retomando los conceptos de Desantes, en relación a los sujetos del Derecho de la Información, para el caso que nos ocupa, se entenderá al sujeto universal como el cliente o usuario de las empresas comerciales, que en un sentido amplio son todos los seres humanos que interactúan con las empresas, tanto en el espacio físico como en el espacio virtual o ciberespacio.

Por su parte, el sujeto cualificado, en relación a las necesidades derivadas de la interacción entre los clientes y las empresas en el ciberespacio, donde convergen varias ciencias, principalmente derecho y tecnología, deberá entenderse como sujeto cualificado a la persona que cuente con conocimientos de derecho y tecnología, pues no es posible tratar de hacer cumplir la ley en un entorno que se desconoce en todo o en parte.

En ese sentido, no es posible que aquellos que no tienen un amplio dominio de la tecnología intenten regular las acciones que se llevan a cabo en la misma, si finalmente los protocolos de comunicación tienen forzosamente que realizar ciertas acciones que a menudo pasan desapercibidas, pero que son inevitables para poder lograr el resultado esperado de la tecnología, a saber, la comunicación o recepción de información, de manera activa (investigando) o de forma pasiva (recibiendo), lo que los sujetos cualificados ponen al alcance del público en general.

En consecuencia, el sujeto cualificado deberá ser un conocedor del derecho, pero además, es necesario tener conocimientos sobre tecnologías como la nube, inteligencia artificial, *Big Data* e *Internet*, solo de esta manera podrá considerarse como un sujeto cualificado del derecho a la información en la sociedad de la información, de tal suerte, que sea apto para poder garantizar la salvaguarda de los derechos de las personas ante la convergencia entre empresas, tecnología, sociedad y gobiernos.

Retomando lo anterior, es de entender que el sujeto organizado deba acumular conocimiento de varias ramas que le permitan desarrollarse libremente en el mercado, sin más restricciones que las que establezcan las leyes. Por ello, es

[58] *Ibidem,* p. 51.

necesario también que se den cuenta de la necesidad de la capacitación para contar con sujetos cualificados que les ayuden a lograr sus objetivos, pero con apego a la normativa, garantizando así el respeto a los derechos humanos ante la triada que conforma la sociedad de la información, a saber, tecnología, sociedad e información.

Respecto al sujeto organizado, en relación con el caso de estudio, debe considerarse a las empresas comerciales, las cuales en su actividad de compraventa de bienes y servicios, requieren tener un alto grado de conocimiento del entorno del mercado, para lo cual deben usar la tecnología que les permita obtener el conocimiento necesario para lograr el éxito esperado, por ende, requieren recolectar, analizar y almacenar información de las personas, además de tener conocimiento de administración, mercadotécnica, informática, derecho, psicología, sociología, por mencionar algunas.

### *2.2. Antecedentes del derecho a la información*

El derecho a la información, que se ha plasmado por primera vez en la *Declaración Universal de los Derechos Humanos de 1948*, es producto de la transformación social posterior a la Segunda Guerra Mundial, pues como ya se ha dicho, el derecho ha de retomar la historia de la humanidad para adaptar o crear nuevas normas que regulen la conducta de las personas.

Este derecho promete brindar mayor certidumbre a la sociedad, permitiendo que puedan acceder a información que les genere conocimiento, así como a difundir sus ideas. Es el inicio de la transición de una época en la que imperaba la opacidad y la incertidumbre, que guiaba a la humanidad por un camino conocido solo para unos cuantos, a una nueva etapa en la que se vislumbra el inicio de la transparencia, de la posibilidad de acceder a la información generada por los gobiernos como resultado de sus actuaciones al servicio del pueblo, así como de la libertad de expresión.

Lo anterior, es un peldaño para la conformación de la llamada sociedad de la información, que no es más que una sociedad más informada, producto de una necesaria evolución social a consecuencia del desarrollo tecnológico, que deriva en la necesidad de adecuar la legislación para que las personas puedan desarrollarse

libremente, hacerse llegar de información que genere conocimiento para mejorar su calidad de vida. Esto, a la luz del derecho a la información que supone que mientras más se sepa de los servidores públicos, mejores elecciones se harán de los mismos, logrando mejorar la calidad de vida de las personas, al menos, eso es lo que se esperaba.

### *2.2.1. Reconocimiento y evolución del derecho a la información*

El derecho a la información se reconoce formalmente a partir de la *Declaración Universal de los Derechos Humanos* en el año 1948[59], que en el artículo 19 contempla que "todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión".

Este artículo refiere que todos tenemos derecho de difundir información haciendo uso de cualquier medio de comunicación, sin embargo, en el año en que se creó este documento aún no cobraban mayor relevancia las tecnologías de la información como medios para difundir informaciones sin limitación de fronteras.

Posteriormente se retoma la idea principal de este artículo para ser plasmado en el artículo 19 del *Pacto Internacional de Derechos Civiles y Políticos*[60] en 1966 que, en el apartado 2 refiere que "Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección".

En este documento ya se definen más claramente los medios de comunicación por los cuales se puede difundir la información y claramente se refiere a los medios de comunicación conocidos hasta el momento, los cuales suponían limitantes en los alcances para la investigación y difusión de información a nivel global. Sin embargo,

---

[59] Adoptada y proclamada por la Asamblea General en su resolución 217 A (III), de 10 de diciembre de 1948, https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf. Consultado: 03/02/2019.

[60] Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966, https://www.ohchr.org/SP/ProfessionalInterest/Pages/CCPR.aspx. Consultado: 03/02/2019.

cabe señalar que al mencionar “cualquier otro procedimiento de su elección”, deja abierta la posibilidad para utilizar los medios tecnológicos emergentes.

Estos medios de comunicación emergentes cambiarían radicalmente la forma de comunicar y difundir información a partir del año 1951, cuando se creó UNIVAC *(UNIVersal Automatic Computer)*, reconocida como la primera computadora que se reprodujo en serie, misma con la que se hicieron las primeras pruebas de comunicación entre dos computadoras conectadas en red.

Posteriormente, en la década de los 60s comenzó el desarrollo de *Internet,* lo cual, como resultado de las investigaciones de innovación, concluyó en el desarrollo de hardware y software, siendo así como surge la conmutación de paquetes, el protocolo TCP/IP así como la computación cliente-servidor, que en un principio se limitaba a conectar grandes computadoras que se encontraban en distintos campus universitarios. Pronto esta tecnología sería retomada por el Departamento de Defensa, así como la Fundación Nacional para las Ciencias con la intención de crear un sistema de comunicaciones militares, proyecto que se denominó ARPANET *(Advanced Research Projects Agency Network)*[61]*,* el cual constaba de una red de computadoras conectadas entre sí, con la finalidad de compartir información de uso militar que ofrecía varias vías para llegar al destinatario de manera mucho más veloz que lo que suponía el envío de un telégrafo o de un mensajero que llevara el mensaje

Esto cobraría mayor relevancia con la creación del proyecto que asumió la Fundación Nacional para las Ciencias (NSF, por sus siglas en inglés), para un *Internet* civil en el año 1986[62]. Sin embargo, no fue sino hasta el años 1989 cuando se haría realidad lo que se había plasmado en la *Declaración Universal de los Derechos Humanos* en el artículo 19, respecto a la difusión de información sin limitación de fronteras, pues con la llegada de la web o *World Wide Web,* creada por Tim Berners-Lee[63], y apoyada del ya mencionado *Internet*, se podía transmitir información de manera global en tan solo unos segundos, de igual manera esta

[61] *Cfr.* Kenneth C., Laudon y Guercio Traver, Carol, *Op. cit*, p. 118–119.
[62] *Cfr. Idem*.
[63] *Cfr. Ibidem*, p. 157.

nueva herramienta tecnológica permitiría ejercer no solo la facultad de difundir información, sino, también de investigar y recibirla de distintas partes del mundo.

El avance de las tecnologías de la información y comunicación se ha planteado como la herramienta para alcanzar una mejor calidad de vida de las personas, dando paso a la denominada sociedad de la información, según la interpretación que hace Alfonso Sánchez de Fritz Machlup. Machlup en su obra *The Production and Distribution of Knowledge in the United States*, en el año 1962, "Utiliza la expresión por vez primera. Define el concepto de 'industria del conocimiento' y explora el conocimiento como un recurso económico"[64].

La implementación de estas tecnologías en la sociedad de la información viene a potenciar las facultades del derecho a la formación, no obstante, aunque estas tecnologías permiten investigar, recibir y difundir información con mayor facilidad y alcance, también se debe dejar en claro que las excepciones de este derecho serán los mismos derechos de las personas que podrían verse afectados por estas prácticas tecnológicas de manera desproporcionada.

Por esto, también es de observar lo que menciona el artículo 12 de la *Declaración Universal de los Derechos Humanos,* respecto a 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 a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."

Podemos observar entonces que los sujetos del derecho a la información son los mismos tres sujetos que menciona Desantes en el Derecho de la Información, con peculiaridades específicas, es decir el sujeto universal corresponde a todas las personas físicas, el sujeto cualificado a los periodistas como los responsables de difundir información de interés social y el sujeto organizado a los medios de comunicación, también conocidos como los *mass media*.

En ese tenor, el sujeto universal es el término que le corresponde a la sociedad en general, es decir a las personas que pueden ejercer las tres facultades del derecho a la información, investigar, recibir y difundir información a través de cualquier medio de comunicación. Sin embargo, al no ser la actividad primaria del

[64] Alfonso Sánchez, Ileana R., *Op. cit.* p. 241.

sustento económico de las personas, se deja la tarea de difundir a los medios de comunicación, los cuales pueden obtener la información de diversas fuentes, incluida la sociedad.

El sujeto cualificado corresponde a aquellas personas que han estudiado una carrera relacionada con las comunicaciones, como el periodismo, ciencias de la comunicación o alguna otra que lo califique como profesional de la información, aunque en la actualidad esto no es un requisito para considerar a una persona como sujeto cualificado en torno al derecho a la información, pues basta con que la persona haga de esta función su fuente de ingreso principal.

Por último, el sujeto organizado, son todas las empresas informativas que se dedican a la difusión de contenidos noticiosos o publicitarios, las cuales pueden tener una personalidad moral o física que tienen como objetivo la difusión masiva de información de interés social.

No obstante, actualmente los medios de comunicación digital y las redes sociales, han permitido que todos los sujetos universales puedan difundir información, incluso hay quienes de manera libre forman sus propias páginas o portales informativos, sin que tengan una carrera relacionada con la comunicación. Esto no significa que esté mal, desde mi punto de vista es una evolución de la misma sociedad y de la tecnología, suceso que el derecho deberá reconocer y ampliar el concepto de sujeto cualificado y de sujeto organizado.

Derivado de ello, se vuelve necesario que los Estados desarrollen todo un entramado jurídico, que permita garantizar tanto el derecho a la información como la protección de otros derechos ante el ejercicio de este derecho, que puede ser ejercido mediante los medios tecnológicos, que actualmente representan uno de los medios de investigación y difusión de información con mayor impacto social y económico.

No obstante, cabe señalar que no por el hecho de dar a conocer sucesos noticiosos, se tenga que dar un reconocimiento de sujeto cualificado a todas las personas que realicen estas prácticas, pues para ello deberán seguir ciertos métodos para la investigación y la difusión de la información que se difunde, ya que de lo contrario podría caer en ciertas violaciones al derecho a la información, sin

darse cuenta o sin que sea la intención de quien en el ejercicio de sus derechos difunda información.

Lo anterior, es importante señalarlo como una introducción al derecho a la información. Sin embargo, en relación al tema que nos ocupa y tomando en cuenta los sujetos del derecho a la información mencionados anteriormente, se puede encuadrar perfectamente a las empresas comerciales como sujetos organizados. Por su parte, el sujeto universal se tomará solo como los seres humanos que pueden, en lo individual o de manera colectiva, ejercer este derecho para investigar información de los productos y de las mismas empresas, recibir aquella información que a su interés convenga respecto a sus intereses de consumo y difundir lo que consideren conveniente con base en sus experiencias de compra, con la única limitante que las leyes contemplen para la protección de los derechos de terceros.

En cuanto al sujeto cualificado, en relación con las empresas y la difusión de la información que estas realizan sobre sus productos y servicios, se debe considerar a las personas con conocimientos de mercadotecnia y marketing, pues serán los más adecuados para hacer la recolección y análisis de información para la generación de nuevos contenidos informativos, enfocados a la venta de los productos y servicios ofertados por las empresas.

Sin embargo, también es necesario que se tengan nociones de psicología conductual, de inteligencia artificial, a manera de conocimiento general, así como de *Big Data* y tecnologías de la nube, con la finalidad de poder trabajar en conjunto con el personal de sistemas y desarrollo de nuevas tecnologías para el logro de los objetivos empresariales.

En resumen, el sujeto cualificado del derecho a la información en relación a las actividades que las empresas realizan, debe ser una persona con conocimiento de mercadotecnia, capaz recolectar y analizar la información mediante el uso de tecnologías como *Big Data*, redes sociales, inteligencia artificial, por mencionar algunas, que permitan generar nuevos conocimientos útiles para el desarrollo de estrategias de mercado en el entorno digital y físico, para lograr los objetivos planteados por la empresa en la sociedad de la información, una sociedad sin fronteras.

De tal manera que también podemos observar que, en relación con el objeto del derecho a la información, en este caso particular, el objeto de protección debe ser el mensaje publicitario, el cual va dirigido al público en general y debe darse a conocer como la información relevante que sea de interés para las personas, la cual debe dar la certeza de que lo que se promete sobre los productos y servicios, sea veraz, tal como lo supone el derecho a la información.

### *2.2.2. Definición de derecho a la información y su introducción en el ordenamiento jurídico mexicano*

En México, el derecho a la información se vislumbra desde la *Constitución de 1847* cuando en su artículo 2° se inserta el texto que menciona: “Es derecho de los ciudadanos votar en las elecciones populares, ejercer el de petición, reunirse para discutir los negocios públicos, y pertenecer a la guardia nacional, todo conforme a las leyes”. Sin embargo, aunque se menciona el derecho de petición, no queda claro a qué se refiere ni ante quién se puede ejercer este derecho. No obstante, tal derecho permite pedir (investigar), y recibir información que se encuentre en posesión de los servidores públicos.

No obstante, en la *Constitución de 1857* se acerca un poco más a lo que se conoce hoy en día como derecho a la información, al insertar en el artículo 8° el texto: “Es inviolable el derecho de petición ejercido por escrito, de una manera pacífica y respetuosa; pero en materias políticas solo pueden ejercerlo los ciudadanos de la República. A toda petición debe recaer un acuerdo escrito de la autoridad a quien se haya dirigido y esta tiene obligación de hacer conocer el resultado al peticionario”.

Es de observar que en esta constitución también se establecen en el artículo 34 los requisitos para que una persona se considere como ciudadano, los cuales son que: […] “teniendo la calidad de mexicanos, reúnan además las siguientes: I. Haber cumplido diez y ocho años siendo casados, ó veintiuno si no lo son. II. Tener un modo honesto de vivir”. De tal manera que todas aquellas personas que no encajen en este supuesto no podrán ejercer este derecho; interpretando este texto, no se puede considerar como un derecho fundamental, pues carece de la universalidad.

De igual manera en el artículo 6° se establece que “la manifestación de ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque la moral, los derechos de terceros, provoque algún delito, o perturbe el orden público”.

En el artículo 7° se establece que “es inviolable la libertad de escribir y publicar escritos sobre cualquier materia. Ninguna ley ni autoridad puede establecer la previa censura, ni exigir fianza a los autores o impresores, ni coartar la libertad de imprenta, que no tiene más límites que el respeto a la vida privada, a la moral y a la paz pública […]”.

Así mismo, en el artículo 9° menciona que: “A nadie se le puede coartar el derecho de asociarse ó de reunirse pacíficamente con cualquier objeto lícito; pero solamente los ciudadanos de la República pueden hacerlo para tomar parte en los asuntos políticos del país. Ninguna reunión armada tiene derecho de deliberar”.

En este artículo constitucional, se encuentra plasmado uno de los derechos que permiten la asociación de personas para desarrollar cualquier tipo de actividades, en el cual, a interpretación, se pueden encuadrar las actividades comerciales, siempre y cuando estas sean lícitas. En la actualidad, las empresas son parte fundamental para el desarrollo económico, y el derecho a la información viene a ser una pieza fundamental para armonizar la convivencia entre las empresas y los usuarios de las mismas, con la intención de que las personas cuenten con la información necesaria que brinde certeza al momento de realizar transacciones comerciales.

La certeza que se busca brindar a los usuarios de las empresas, va más allá de solo dar la información referente al costo del producto, pues es necesario que también se le indiquen los mecanismos establecidos para hacer valer la garantía cuando esto sea necesario, así como qué datos serán recolectados, con qué finalidades, las medidas de protección con que contarán dichos datos y los derechos con los que cuentan las personas para controlar el uso de los mismos. Todo esto se engloba dentro del derecho que toda persona tiene a recibir información veraz y oportuna, elemento fundamental del derecho a la información.

Posteriormente, en la *constitución de 1917*, se retoman los mismos conceptos respecto a la libertad de escribir, la libertad de manifestación de las ideas y se modifica el artículo 8° que corresponde al derecho de petición, que refiere que:

> Los funcionarios y empleados públicos respetarán el ejercicio del derecho de petición, siempre que ésta se formule por escrito, de una manera pacífica y respetuosa; pero en materia política, sólo podrán hacer uso de ese derecho los ciudadanos de la República.
> A toda petición deberá recaer un acuerdo escrito de la autoridad a quien se haya dirigido, la que tiene obligación de hacerlo conocer en breve término al peticionario.

Por su parte el artículo 9° también se modifica agregando el texto que refiere que, "No podrá considerarse ilegal, y no podrá ser disuelta una asamblea o reunión que tenga por objeto hacer una petición o presentar una protesta por algún acto, a una autoridad", siempre y cuando no se recurra a la violencia y a las amenazas para obligar a la autoridad a resolver la controversia.

Así entonces, podemos observar que desde 1857, las personas ya tenían un derecho a la información, mediante el derecho a la libertad de expresión que permitía la difusión de información. Aunado a ello, la libertad de imprenta permitía que las ideas se difundieran por medios impresos sin previa censura y se podía acceder a la información pública mediante el derecho de petición. Aunque de forma limitada, ya se contaba con la base del derecho a la información en esta constitución.

Sin embargo, el derecho a la información viene a tomar mayor fuerza a partir de la *constitución de 1977*, cuando se introduce en la parte final del artículo 6° el texto, "el derecho a la información será garantizado por el Estado". Esto significa que el Estado deberá adecuar las leyes para que las personas puedan ejercer libremente las facultades de investigar, recibir y difundir información sin censura previa y sin ser molestados a causa de la información que en el ejercicio de estas facultades difundan por cualquier medio de comunicación, y tendrán la garantía del Estado para que nadie pueda coartar dicho derecho.

Varios años después, ya en el año 2002, se promulga la *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental,* la cual garantiza el derecho de acceso a la información en posesión de los entes de gobierno, dicho

derecho es una variante del derecho a la información que regula específicamente el acceso a la información en posesión de los entes de gobierno, con la intención de que los gobernados conozcan el destino de los recursos económicos del erario público.

En ese mismo año se creó el Instituto Federal de Acceso a la Información Pública, para desempeñar la función de garante del derecho de acceso a la información pública. Cabe aclarar que sobre este derecho no se ahondará por ser un tema de estudio distinto al que se pretende en este trabajo, solo se menciona a manera de antecedente en la rama del derecho a la información en relación a la inserción de la parte final del artículo 6° constitucional en 1977.

Desde esa fecha a la actualidad, se han realizado varias reformas al artículo 6° constitucional, No obstante, en relación al derecho a la información no se le han hecho cambios, pues dichas reformas han consistido mayormente en adecuar la legislación en materia de trasparencia y acceso a la información en posesión de las instituciones de gobierno.

Así, habiendo reconocido este derecho en la Constitución y vía el artículo 133, se ha logrado que, por mandato constitucional, la legislación internacional a través de los tratados y pactos, tenga vigencia también en México, aún por encima de las leyes estatales y solo por debajo de la constitución. Esto ha permitido que poco a poco la constitución se vaya adecuando a la normativa jurídica internacional, haciendo cada vez más tangible el derecho a la información.

Consecuentemente, el derecho a la información es un derecho que tiene una carga negativa y una positiva con relación al Estado, es decir que este derecho se ejerce de manera voluntaria sin que la ley o el gobierno lo exija, pero a la vez es un derecho que el Estado está obligado a garantizarle a la sociedad.

De tal manera que la labor de los juristas ha sido plasmar los derechos de las personas, las excepciones de dicho derecho y las obligaciones del Estado para garantizarlo. Encontrando como excepciones los mismos derechos humanos en donde la afectación del ejercicio del derecho a la información pueda causar algún daño a terceros o transgredir algún otro derecho; para ello se deberá hacer una ponderación de derechos en aras de resolver en los mejores términos sin afectar

los derechos, o en su caso optar por la solución que resulte menos perjudicial para los derechos de las personas en cuestión.

Sin embargo, aunque las leyes contemplan este derecho y aun cuando tiene ya un largo recorrido en la legislación mexicana e internacional, sigue siendo un derecho que parece ser de privilegio, pues solo algunos lo ejercen plenamente; mayormente los periodistas y aquellas personas que están allegadas a los círculos políticos, incluso, Leonel García Tinajero menciona que: "[…] las disposiciones en materia de derecho a la información no responden de modo integral a las necesidades del conjunto de relaciones que abarca, ya sea por ignorancia o por intereses creados"[65].

Es por ello que el derecho a la información aún sigue siendo un tema de estudio que ha llevado a numerosas conclusiones sobre lo que es este derecho, sin embargo, una de las conclusiones que parecen más adecuadas, después del análisis de varios artículos y algunos libros, en donde se trata de definir y hacer entender este derecho, es la definición que hace Sergio López Ayllón, quien refiere que el derecho a la información:

> […] consiste en que cualquier individuo puede, con relación al Estado, buscar, recibir o difundir —o no buscar, no recibir ni difundir— informaciones, opiniones e ideas por cualquier medio; y que ese individuo tiene frente al Estado un derecho a que éste no le impida buscar, recibir o difundir —o no lo obligue a buscar, recibir o difundir— informaciones, opiniones e ideas por cualquier medio[66].

Actualmente, los medios que permiten hacer difusión, investigación y recepción de información, son muy diversos y de gran impacto social, por lo que, es necesario que este derecho evolucione en busca de una regulación más allá de lo que se ha dicho en papel, pues el objetivo de este derecho es tener una sociedad mejor informada y capaz de tomar decisiones que guíen el rumbo de las naciones como efecto del conocimiento y la circulación de opiniones e ideas.

---

[65] García Tinajero, Leonel, "El Monopolio Mediático en México: toque de queda al derecho a la información", en Ponce Báez, Gabriela y García Tinajero, Leonel (coord.), *Las Fronteras del derecho de la información,* México, Novum, 2011, p. 7.

[66] López Ayllón, Sergio, "Democracia y Acceso a la Información", *Colección de cuadernos de Divulgación sobre Aspectos doctrinarios de la Justicia electoral, No. 9*, Edit. Tribunal Electoral del Poder Judicial de la Federación, México, 2005, p.29.

Lo anterior, a consecuencia del avance de las nuevas tecnologías como la inteligencia artificial y el *Big Data,* parece ser solo un ideal, pues con estas tecnologías, contrario a lo que se esperaba de ellas en relación a la capacidad para informarse de mejor manera sobre temas de interés social, se ha limitado el conocimiento al recibir información cada vez más adecuada a nuestro perfil digital, a nuestras búsquedas anteriores o a nuestras aficiones e intereses personales, limitando el conocimiento a un círculo vicioso creado por nosotros mismos, en el que nos encontramos atrapados a consecuencia de nuestra huella digital, que predice de manera arbitraria nuestros pensamientos e intereses.

No obstante, para el caso que nos ocupa, este derecho se analiza en torno a las empresas comerciales, las cuales se consideran como el sujeto organizado, entendiendo al sujeto organizado en este estudio y en relación al derecho a la información, como las empresas que recolectan y tratan datos personales para adecuar sus acciones comerciales y que por ende, deben difundir la información pertinente para que los usuarios puedan decidir libremente y de manera informada sobre los datos que han de proporcionar a las empresas, para que finalidades, así como decidir sobre qué productos adquieren acorde a los beneficios prometidos por la empresa oferente.

Esto supone que las empresas deberían informar sobre el uso de las tecnologías mencionadas anteriormente y con qué finalidades las usarán. Aunque las empresas a menudo informan esto de manera muy superficial, parece que el problema mayor radica en la cultura y el conocimiento de la sociedad que no comprende lo que sucede, como ya se ha mencionado anteriormente, estas tecnologías realmente terminan decidiendo que queremos conocer y como lo queremos conocer, violando de cierta manera el derecho al libre desarrollo de la personalidad.

A manera de conclusión respecto al derecho a la información, para el caso que nos ocupa, se deben entender las facultades del derecho a la información como las facultades que las personas tienen para investigar información referente a los productos que las empresas ofertan, los costos, los beneficios, la calidad, los mecanismos para hacer válida la garantía en caso de que aplique, la rapidez, etc. Todo aquello que brinde certeza y tranquilidad al cliente, así como lo referente a las

condiciones del tratamiento de los datos personales. En relación con el Estado, debe existir una carga positiva que garantice que las personas reciban información veraz, no engañosa y de manera oportuna para la toma de decisiones.

Por su parte, la facultad de recibir, en relación a la información que difunden las empresas, tiene una carga negativa en relación al Estado, pues este no puede obligar a las personas a recibir ningún tipo de publicidad o información, pues esto es decisión personal, y cada persona decidirá qué información de la que las empresas ponen a su alcance, es de su interés, en cuyo caso, será receptivo ante dicha información, de lo contrario tiene la libertad para no recibirla e incluso en medios digitales, puede ejercer esta facultad para pedir a la empresas en cuestión, el cese del envío de publicidad.

La facultad de difundir tiene una carga tanto positiva como negativa en relación con el Estado, pues este debe garantizar que exista la libertad de difundir las ideas, pero a su vez no puede obligar a las personas a hacerlo. Así entonces, esta facultad es de vital importancia para las empresas en relación con sus clientes, pues en la actualidad y ante la proliferación de medios de difusión de información, las personas pueden hacer viral cualquier tipo de información, la cual en ocasiones puede ser favorable para las empresas y en otras, totalmente desfavorable.

Por ello, las empresas deberán cuidar cada vez más la calidad de sus productos y servicios, mejorar el acompañamiento para poder generar lealtad, ser competitivos y mantenerse siempre a la vanguardia, así, se aumenta la probabilidad de que la información que los usuarios difundan acerca de sus productos sea favorable.

Lo anterior no sería posible sin la implementación de la tecnología para el análisis de información y establecer relación con los clientes, abrir espacios de opinión en donde el cliente sienta la libertad que este derecho promete y así, juntos, empresas y sociedad, caminar hacia una mejor calidad de vida como se esperaba sucediera en la sociedad de la información.

Parece de vital importancia que el derecho a la información contemple el acceso a las nuevas tecnologías, a la banda ancha y al *Internet,* pues, aunque con sus limitantes y confusiones respecto a la tecnología –banda ancha e *Internet*– se contemplan dichas herramientas tecnológicas que, a interpretación, más que ser un

derecho en sí mismas, son herramientas que permiten el ejercicio de otros derechos, en específico, los derechos que convergen con la información.

*2.2.3. Excepciones del ejercicio al derecho a la información*

El derecho a la información no puede considerarse como un derecho absoluto, pues si bien es cierto que es un derecho que dota de facultades a las personas para poder investigar, recibir y difundir información, encuentra sus excepciones en los mismos derechos de terceros, como son el derecho a la propia imagen, a la intimidad, a la privacidad, la dignidad, la moral y la protección de datos personales.

En lo que respecta a las facultades del sujeto universal, este no puede, en el ejercicio de la facultad de investigación, obtener información que la empresa resguarda bajo cualquier mecanismo de seguridad y en los términos que el derecho a la propiedad industrial o intelectual, contempla para garantizar el goce y disfrute de los bienes morales y patrimoniales de sus creaciones.

Así entonces, en el ejercicio de investigación, no se podrá transgredir el espacio íntimo de las personas para poder obtener información que les concierne a su vida privada. Sin olvidar que, dependiendo de la función que desempeñe cada persona, podrá disminuir su esfera íntima, sin que esto signifique que pierda el derecho a conservar aspectos de su vida personal en desconocimiento de terceros y que nadie podrá, en el ejercicio de su derecho a la información, transgredir este derecho.

Las personas que desempeñan cargos públicos se consideran personas públicas, y por este hecho su esfera de protección a la privacidad y a los de más derechos relacionados con la personalidad disminuye, por tratarse de una persona que se considera un empleado de la sociedad, sobre quien se debe tener conocimiento para poder exigir cuentas de su actuar y del ejercicio de los recursos del pueblo.

Las personas de notoriedad pública, entendidas como los artistas u otras personas que son reconocidas entre la sociedad, pero que no son personas públicas, aunque en menor grado, también disminuye su esfera de protección a los derechos de la personalidad, pues al ser personas de interés para algunos cuantos,

también están sujetos al escrutinio social, a la crítica y a la opinión pública que se da como característica de toda sociedad democrática.

Por su parte, el ejercicio de la facultad de difundir información, el cual está mayormente relacionada con las labores de los informadores (periodistas), no se podrá difundir información que concierna a la vida íntima de las personas, ya que, de hacerlo, esto supondría una invasión a la privacidad de la persona y podría repercutir directamente sobre su dignidad. En relación a las empresas, esto podría repercutir en su imagen pública y, por lo tanto, en su patrimonio económico y como tal, corresponde la reparación del daño patrimonial.

Así, en el ejercicio de esta facultad, los informadores también ejercen el derecho del secreto profesional del periodista, el cual por un lado es un derecho ante las autoridades judiciales o administrativa y ante su mismo jefe de la empresa informativa, pero que a su vez constituye un deber como excepción del derecho a la información al obligar a los periodistas a no difundir aquella información que pueda poner en riesgo la seguridad nacional, que pueda desencadenar caos o que pueda atentar contra la integridad de la fuente informante.

Sin embargo, también les da la facultad para difundir aquella información que es de interés social y garantizar la seguridad de la fuente que haya proporcionado dicha información. Por ejemplo, cuando alguna empresa está poniendo en riesgo la salud de las personas o el medio ambiente debido a las actividades de producción y/o transformación de materias, en cuyo caso, los más adecuados para hacer circular la información, deberán ser los medios de comunicación.

Por su parte, quienes den a conocer la información, deberán hacer una investigación más profunda sobre el tema, con la intención de verificar los hechos antes de darlos a conocer, pues en caso de que dicha información no sea confirmada, podrían enfrentar cargos de reparación del daño.

El ejercicio de la facultad de difundir información supone también un componente ético y de valores humanos, para que no se dé a conocer información falsa como hechos verdaderos en beneficio de ciertos grupos sociales o políticos, aún a sabiendas que no es información veraz. En el caso que nos ocupa, esto aplica a la veracidad de la información publicitaria que las empresas difunden, pues lo que

prometen con sus productos y servicios debe ser veraz, es decir, no deben engañar a las personas por el interés económico que supone la venta de sus productos y servicios.

Recordemos que el derecho a la información no considera como objeto de protección aquellos mensajes que se den a conocer como hechos reales aun sabiendo que son falsos, así como aquellos mensajes que se emitan con la intensión de dañar la moral, la reputación, la honra o la dignidad de las personas. Así, sujetos organizados y sujetos universales, deberán actuar de manera ética y consciente, sabidos que la difusión de información falsa, puede repercutir en perjuicio de la relación de convivencia en sociedad.

La facultad de recibir información contempla al sujeto universal como actor pasivo ante la información, haciéndose llegar de ella mediante los medios de comunicación, sin tener la necesidad de investigar y contrastar opiniones, experiencias e ideas del público o de distintas fuentes informativas para validar la información que se está dando a conocer. Como se dijo anteriormente, el sujeto universal podrá solicitar el cese del envío de información a sus medios digitales, así como ignorar aquella que se difunde en el entorno físico cuando no la considere de interés.

Por su parte esta facultad, ejercida por los sujetos organizados supone un componente ético, al no considerar como un acto ético la difusión de los datos que se les haya proporcionado como consecuencia de una transacción comercial. Por otro lado, cuando se trata de información que puede evitar una tragedia o que puede ayudar al esclarecimiento de un delito o la prevención de una catástrofe, la persona que haya recibido esa información, aun bajo juramento de secrecía deberá darla a conocer a las autoridades competentes para evitar la comisión de algún delito, para prevenir catástrofes o pandemias.

Estas facultades, derechos y obligaciones, configuran también las excepciones del derecho a la información, ya que de ello depende en qué situaciones concretas el derecho a la información debe ceder ante otros derechos, que de no ser protegidos podrían repercutir en mayor detrimento para la persona, de lo que podría ocasionar la excepción del derecho a la información.

*2.3. Definición y concepto del derecho a la protección de datos personales*

El derecho a la protección de datos personales es la respuesta a la proliferación de las tecnologías de la información y comunicación, a partir de que las computadoras comenzaron a tomar importancia para las empresas por las capacidades para la recolección y procesamiento de información, y más aún con la llegada del *Internet* en el año 1969, pues esta nueva tecnología permitiría que todas las personas que tuvieran acceso a una computadora, podrían transferir información a cualquier parte del mundo. Sin embargo, también podrían vulnerar los derechos que se habían plasmado en la *Declaración Universal de los Derechos Humanos de 1948.*

Lo anterior, dejó ver que estábamos ante una tecnología que, si bien incrementaría el desarrollo económico al permitir hacer negocios con empresas de otras naciones, gracias a la nueva forma de comunicación a distancia, además de permitir concebir una sociedad mejor informada, también vislumbraba un agujero negro respecto a donde puede llegar a parar la información de las personas al ser transmitida, lo cual, sin duda, puede ser riesgoso para la salvaguarda de la seguridad e integridad física de las mismas.

Respondiendo a este nuevo reto, el estado de *Land de Hesse* en la República Federal de Alemania, se creó la primera ley sobre protección de datos personales, misma que daría la pauta para la creación de las próximas leyes que habrían de replicarse con sus respectivas adecuaciones a lo largo y ancho del planeta, con sus excepciones, claro está. Así, varios años más tarde, México se suma a los países que cuentan con leyes sobre protección de datos personales, bajo los principios generales que regulan su protección en el mundo, con el objetivo de garantizar la protección de la privacidad ante el uso de las tecnologías de la información y comunicación en la sociedad de la información.

En México, el reconocimiento constitucional del derecho a la protección de datos personales como un derecho humano, se vislumbra desde la reforma al artículo 6° en julio de 2007. Sin embargo, todavía está regulado dentro del derecho de acceso a la información pública, pues en este momento la única Ley a la que se refiere la fracción II del mencionado artículo constitucional, es la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, por lo que aún no

se puede considerar el derecho a la protección de datos personales como un derecho autónomo.

Es importante mencionar que, aunque en México había algunas entidades federativas como Colima, Guanajuato, Oaxaca y México, D.F., que antes de que existieran la Ley Federal y General sobre Protección de Datos Personales, ya contaban con una ley específica para la protección de los datos personales.

Sin embargo, a nivel federal, no es sino hasta junio del año 2009 que el derecho a la protección de datos personales alcanza su reconocimiento constitucional como un derecho humano autónomo, adicionando en esta reforma al artículo 16° el texto que a continuación se presenta:

> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros[67]

A partir de esta reforma, ya con un reconocimiento constitucional, se puede decir entonces que las personas cuentan con un nuevo derecho que les permite tener el control de sus datos personales, y que este nuevo derecho otorga la libertad para autodeterminarse, es decir, la libertad de decidir a quién le proporcionan sus datos personales una vez le hayan sido informados los términos y condiciones de su tratamiento, lo cual supone la previa información por parte del responsable respecto al tratamiento de los mismos, las finalidades y la seguridad con la que cuentan, de tal manera que el titular tenga los elementos suficientes para que, de manera consciente, decida a quién y para qué proporciona sus datos.

De esta forma, la protección de datos personales supone una sana convivencia entre la tecnología, el comercio y la protección de la privacidad e intimidad de las personas, marcando límites, deberes y obligaciones en el tratamiento de datos personales que, bajo libre consentimiento y aceptación debidamente informado, los

[67] Reforma publicada en el DOF el 01-06-2009, http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_187_01jun09.pdf. Consultado: 05/03/2019.

titulares, hayan proporcionado como requisito para realizar alguna transacción comercial. A esta facultad para decidir sobre los datos personales, se le ha denominado autodeterminación informativa.

Gracias a ello, las personas pueden disponer de la información que de su persona exista en los registros de bases de datos; ello, a fin de que dicha información sea veraz, íntegra, actualizada, no intrusiva y con las garantías de seguridad pertinentes conforme a la finalidad para la cual hayan sido recolectados[68].

Por otra parte, el derecho a la protección de datos personales garantiza que, aquellas promesas en cuanto al tratamiento de datos personales, se cumplan conforme a lo convenido en el aviso de privacidad. Además de que, da las facultades al titular para poder acceder a sus datos, rectificarlos en caso de ser necesario, cancelarlos cuando así lo permita la relación contractual entre el particular y el titular, así como la posibilidad de oponerse al tratamiento de los datos personales en los términos establecidos por la Ley.

Entonces, el derecho a la protección de datos personales es un derecho autónomo y abarca los derechos de acceso, rectificación, cancelación y oposición, (Derechos ARCO). Así como también la autodeterminación informativa, que en conjunto permiten al individuo tener el control de sus datos personales y, por ende, garantizar el respeto a su privacidad e intimidad. En resumen, el derecho a la protección de datos personales se lee de la siguiente manera:

> Es la facultad que otorga la Ley para que tú, como dueño de los datos personales, decidas a quién proporcionas tu información, cómo y para qué; este derecho te permite acceder, rectificar, cancelar y oponerte al tratamiento de tu información personal. Por sus iniciales, son conocidos comúnmente como derechos ARCO (INAI n.d.)[69].

---

[68] Aveleyra, Antonio M. 2003. “El Derecho de Acceso a la Información Pública vs. el Derecho de Libertad Informática”. *Jurídica-Anuario, Revista de la Universidad Iberoamericana* (32): 403–443. https://revistas-colaboracion.juridicas.unam.mx/index.php/juridica/ article/download/11488/10520. Consultado: 08/03/2019.

[69] INAI, ¿En qué consiste el derecho de protección de datos personales?, http://inicio.ifai.org.mx/SitePages/Como-ejercer-tu-derecho-a-proteccion-de-datos.aspx?a=m1. Consultado: 11/03/2019.

Si bien es cierto que, en la actualidad, las múltiples leyes que existen en el país respecto a la protección de datos personales, en lugar de facilitar el ejercicio de este derecho a los titulares, parece dificultarlo. No obstante, para el tema en cuestión, este derecho se analiza en torno a la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* lo que deja fuera del estudio, la ley general y las leyes estatales en materia de protección de datos personales en posesión de los sujetos obligados.

A partir de esto, nos adentraremos en el tema de la protección de datos personales, para lo cual, es necesario saber también cuáles son las esferas de la personalidad como ejes centrales de protección de este derecho y como estas interactúan en el entorno social. Para ello, comenzaremos haciendo una diferenciación entre privacidad e intimidad, para, posteriormente relacionar las nuevas tecnologías con estos derechos y, finalmente, revisar los principios, deberes y obligaciones que regulan las acciones de las empresas en el tratamiento de datos personales, para garantizar el respeto a los derechos de la personalidad en su interacción con los clientes.

### *2.3.1. Privacidad e intimidad*

Algunos autores hacen referencia a los términos privacidad e intimidad como sinónimos, sin hacer distinción alguna, aludiendo a ellos como el derecho que conlleva al derecho de disfrutar de la vida personal y a ser dejado en paz o en soledad consigo mismo, Emilio Pfeffer Urquiaga menciona que:

> Como derechos de la personalidad, la intimidad o privacidad, el honor y la imagen, son valores o derechos fundamentales que sirven de presupuesto para el ejercicio de otros derechos. En tal sentido son esenciales, originarios e innatos, extrapatrimoniales, intransmisibles, oponibles «erga omnes», irrenunciables e imprescriptibles y, en principio, intransferibles.[70]

Por su parte Ernesto Villanueva y Vanessa Díaz, mencionan que “toda persona tiene derecho a vivir su propia vida, a desarrollarse conforme pueda y pretenda, a

[70] Pfeffer Urquiaga, Emilio, Los derechos a la intimidad o privacidad, a La honra y a la propia imagen. Su protección frente a la libertad de opinión e información, Ius et Praxis, núm. 1m vol. 6, 2000, p. 465, http://www.redalyc.org/pdf/197/19760123.pdf. Consultado: 15/07/2017.

generar relaciones con otros o a mantenerse ajeno y en soledad"[71], asimismo mencionan que la privacidad, "[…] tiene un sentido activo que tiende a concretar la protección de los particulares impidiendo que terceros se ocupen de la vida privada de otros"[72].

María de los Ángeles Guzmán García, en su tesis doctoral denominada *El derecho fundamental a la protección de datos personales en México: Análisis desde la influencia del ordenamiento jurídico español,* respecto a la privacidad menciona que:

> El estudio de la privacidad, parte de un derecho pasivo proclamando la "no injerencia en la vida privada" del individuo y se sitúa en el catálogo de los derechos de primera generación. Este derecho llega a reivindicar un derecho de libertad informática o control de los datos personales incluidos en un fichero informático[73].

Sin embargo, hasta aquí aún no queda claro si la privacidad y la intimidad son lo mismo o si deben considerarse como derechos distintos. Para ello, es necesario revisar lo que se menciona en el artículo 12 de la *Declaración Universal de los Derechos Humanos* de 1948, en el cual se lee, "Nadie será objeto de injerencias arbitrarias en su *vida privada*, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

En ese mismo sentido, la *Constitución Política de los Estados Unidos Mexicanos*, en el artículo 6°, inciso A, párrafo II, menciona que "la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes"[*74*]. Como ya se ha mencionado anteriormente, la única ley que regulaba el tratamiento de datos personales, era la *Ley Federal de*

---

[71] Villanueva, Ernesto y Díaz Vanessa, *Derecho de las Nuevas Tecnologías*, México: Oxford University Press México, 2015, eBook.
[72] *Idem.*
[73] Guzmán García, María de los Ángeles, *El derecho fundamental a la protección de datos personales en México: Análisis desde la influencia del ordenamiento jurídico español,* Universidad Complutense de Madrid, 2013, p. 60, https://eprints.ucm.es/22817/1/T34727.pdf. Consultado: 12/04/2019.
[74] Reforma publicada en el DOF el 20-07-2007, http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM _ref_174_20jul07_ima.pdf. Consultado: 13/04/2019.

*Transparencia y Acceso a la Información Pública Gubernamental,* por lo que aún no estamos hablando de un derecho humano reconocido en la Constitución.

De acuerdo a lo anterior, se puede decir que la privacidad es un derecho que protege la voluntad de las personas a desarrollarse libremente en sociedad, a relacionarse o no, con terceras personas o a permanecer en soledad sin ser molestados y a que nadie intervenga en su vida privada, es decir, que no haya injerencias de terceros en aquellos asuntos que solo competen a la vida privada de las personas.

Como es de notar, en ninguno de estos instrumentos jurídicos se habla de la intimidad, por lo que parece que cuando se alude a la intimidad, se remite a la privacidad. No obstante, es necesario diferenciar entre estos dos derechos, puesto que más adelante se llevarán estos términos al terreno de los datos personales, y es de suma importancia poder diferenciar lo privado de lo íntimo.

Como ya se ha dicho anteriormente, la Constitución mexicana no menciona la intimidad como un derecho. No obstante, algunos autores si, se han ocupado del tema y aunque parece compleja la tarea de diferenciar entre privacidad e intimidad, podemos retomar lo que menciona Ernesto Villanueva y Vanessa Díaz, quienes estipulan que:

> La intimidad es el derecho a no ser conocidos, en ciertos aspectos por los demás. Es un derecho al secreto, a que los demás no sepan lo que somos o lo que hacemos. En ese mismo sentido, anidan otras cuestiones que vinculan como derechos personalísimos, tales como el honor, la imagen, la dignidad el perfil frente al público o la opinión personal que de uno se tiene, etc.[75]

María de los Ángeles, en la tesis citada, menciona que; “El derecho a la intimidad se caracteriza por un eminente contenido negativo para salvaguardar del conocimiento ajeno una parte de nuestra vida personal y familiar, es decir, aquella que deseamos tener en el lado más reservado o secreto de nuestra vida.[76]

Mientras que Mariana Cendejas Jáuregui, afirma que “La palabra intimidad, de acuerdo con el diccionario de la Real Academia Española, se refiere a la zona

[75] Villanueva, Ernesto y Díaz Vanessa. *Op. Cit.* p. 723
[76] Guzmán García, María de los Ángeles, O*p. Cit.* p.118.

espiritual, íntima y reservada de una persona o de un grupo, especialmente de una familia".[77]

Así entonces, se puede decir que la intimidad es un derecho que permite a la persona desarrollarse libremente en su esfera personal, manteniendo en reserva del público, sus pensamientos, sus creencias religiosas, sus gustos, su afiliación política, etc. Cuestiones que solo pueden ser compartidas a voluntad de la persona, en el entorno familiar o íntimo, impidiendo así que terceras personas tengan conocimiento de temas que podrían propiciar el odio o la discriminación de la persona.

Cabe señalar en este punto, que el uso de las tecnologías que ya se han mencionado con anterioridad, pueden violar este derecho al dar como resultado del análisis de información, el conocimiento de aspectos íntimos de la personalidad, como la afiliación política, las creencias religiosas, los pensamientos y gustos, los cuales encajan en el terreno de los datos sensibles, es decir aspectos de la intimidad de las personas.

Como hemos visto, el derecho a la privacidad y el derecho a la intimidad, están estrechamente ligados y es de entender que exista tal confusión al momento de diferenciarlos. Sin embargo, es notorio que ambos derechos buscan la protección del libre desarrollo de las personas, sin que terceros intervengan en su vida personal, permitiendo que la personas sea dueña de su propia vida, de sus decisiones y se autodetermine respecto a qué aspectos de su vida mantiene en la esfera privada y cuales en la esfera íntima.

A manera de ejemplo para diferenciar entre privacidad e intimidad, se presenta la figura 2.1, en la que se ilustra el entorno social en el que se desenvuelven las personas, así como las esferas de derechos intrínsecos a la persona y que deben ser protegidos por el Estado; sea de manera negativa o positiva, es decir permitiendo a la persona decidir libremente sobre sí mismo o garantizando que no existan injerencias arbitrarias hacia su persona, que se le obligue a proporcionar información respecto a su vida privada, o que de manera arbitraria se conozca

[77] Cendejas Jáuregui, Mariana, Manual de Autoformación sobre la Ley de Protección de Datos Personales para el Distrito Federal, México: Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, p. 24.

información más allá de la que es estrictamente necesaria para su desenvolvimiento en sociedad, la cual supone la interacción con las empresas y entre iguales.


Figura 2.1. Esferas de derechos de la persona en el entorno social
*Fuente: Elaboración propia*

En esta ilustración podemos observar que en el entorno social en el que las personas –seres humanos– se desarrollan, puede existir un sinnúmero de personas que son sujetos de derechos, cada una con personalidad propia y que ejerce de manera distinta sus derechos; entre los cuales podemos mencionar los que competen a la protección de datos personales, tales como, la seguridad e integridad física, el honor, la dignidad, la propia imagen, la reputación e intimidad.

Todos estos derechos permiten el libre desarrollo de la personalidad, dejando a voluntad de la persona el grado de ejercicio de los mismos en el sentido de que cada quien podrá autodeterminarse respecto a qué partes de su vida privada pone al descubierto y en conocimiento del resto de las personas que forman parte del entorno social en el que se desarrolla.

De tal manera que las actividades que la persona realice en sociedad podrán determinar la honorabilidad, la dignidad y la reputación de la misma, así como el uso que de su imagen permita o haga por cuenta propia, pero que finalmente son

aspectos de su vida privada que deben ser compartidos con el resto de la sociedad para poderse relacionar y desarrollarse libremente como persona.

Ahora bien, los aspectos de la intimidad como esfera sensible, no suponen la necesidad de ser compartidos con nadie más como requisito para la convivencia social, pues son aspectos que solo conciernen a la persona y la reserva de los mismos no supone una limitante para su desarrollo en sociedad.

Desde esta perspectiva, los datos personales deben separarse en tres grandes grupos; los datos generales o de identificación, es decir los datos que se requiere compartir a diario para poder desarrollarse en sociedad y que suponen la necesidad de compartir ciertos datos personales para el intercambio de bienes y servicios; los datos patrimoniales y financieros, los cuales solo en casos específicos se tendrán que compartir con terceros para el cumplimiento de las finalidades para las que se recolectan y, por último, los datos personales sensibles que solo en casos excepcionales se tendrán que proporcionar a terceros o con las empresas comerciales.

Así entonces, se puede decir que los datos personales son los que se comparten a diario cuando hacemos transacciones comerciales, bancarias, cuando nos registramos a algún curso, etc. Sin agotar aquí las posibles opciones que implican compartir datos personales que recaen en la esfera privada y que, por ende, deben ser protegidos por la ley, sin que ello suponga limitar su circulación para el libre desarrollo de la personalidad, para el desarrollo económico y para el ejercicio de otros derechos.

Debemos tener en cuenta que esos datos personales que corresponden a la esfera privada de la persona, deben ser compartidos para poder generar relaciones sociales. Sin embargo, debe existir la voluntad de la persona para poder compartirlos bajo ciertas condiciones que le permitan tener un control de quién, y para qué, conserva esos datos, con la finalidad de proteger los demás derechos que convergen en la esfera de lo privado, tales como el derecho al honor, el derecho a la honra, el derecho a la propia imagen y el derecho a la reputación.

Sin embargo, la intimidad, como se ve en la imagen, es un derecho que se ha colocado como centro de la privacidad, el cual determina la personalidad del

individuo derivado de sus creencias, su espiritualidad, su orientación sexual, su estado de salud, su afiliación política, y depende de ello la manera en que decide relacionarse con las demás personas, sin que esto le impida insertarse en sociedad de manera igualitaria al resto de la comunidad.

Debido a que estos datos no son necesarios para relacionarse en sociedad ni para realizar transacciones comerciales o de cualquier otra índole, la persona tiene el derecho de reservar dichos datos para el entorno familiar o guardarlos para sí mismo, esto le garantiza la no injerencia de los demás en su intimidad, evitando con ello ser víctima de discriminación o de actos de odio por su condición sexual, creencias religiosas o su estado de salud.

Dicho lo anterior, estamos en posibilidad de identificar la diferencia entre privacidad e intimidad. Así entonces, debemos entender que la privacidad es el derecho que engloba otros derechos entre los cuales se encuentra la intimidad, y que este último, por tratarse de un derecho personalísimo en el que ni el Estado ni terceras personas deben intervenir, requiere de especial protección contra tales injerencias, por ello, aunque debe ser tratado dentro del derecho a la privacidad, se debe poner especial atención en cuestiones que puedan afectar la intimidad de la persona.

En resumen, la privacidad es la esfera general de la persona, en ella convergen varios derechos intrínsecos a los seres humanos y que deben ser protegidos por el Estado, sea de manera positiva o negativa, es decir, permitiendo hacer o no obligando a hacer aquello que las personas no deseen hacer.

Por su parte, la intimidad es la esfera más íntima de la persona, en la cual convergen todos los datos sensibles, es decir, aquellos datos que no son necesarios para el libre desarrollo en sociedad, datos que solo a voluntad del titular podrán ser dados a conocer en su entorno familiar o con amigos de confianza. Hay que insistir en que la secrecía de estos datos no impide insertarse en sociedad y la difusión de los mismos podría derivar en la discriminación, motivo por el que deben ser tratados bajo estrictas normas de seguridad, y solo con el consentimiento expreso y por escrito del titular de los mismos.

Es aquí donde toma especial relevancia el uso de las tecnologías de la información y comunicación, pues el análisis automatizado con sistemas de inteligencia artificial aplicados a la información que el *Big Data* permite recolectar y analizar, puede dar un perfil de las personas que revele datos de esa esfera tan protegida, lo cual supone una injerencia arbitraria a lo más profundo de su vida privada, su intimidad.

Por tal motivo, es de interés retomar los sujetos a los que nos hemos venido refiriendo anteriormente, estableciendo precisiones para este caso en relación a la protección de datos personales, al sujeto cualificado, pues con respecto al tema, los sujetos universal y organizado no tendrán diferencias al vincularlos a este derecho.

Antes de comenzar a hablar de los sujetos, es importante también dejar en claro que en relación a este derecho y de acuerdo los sujetos del mismo, es de interés mencionar el objeto del derecho. Así entonces, el objeto del derecho a la protección de datos personales no son los datos personales *per se.* No obstante, los sujetos son los ya mencionados con anterioridad, con sus respectivas adecuaciones al tema.

De tal manera que, aunque pareciera que el objeto del derecho a la protección de datos personales son los mismos datos, en realidad no es así, pues no debemos olvidar que éste, al igual que otros derechos, está centrado en la protección de la persona como individuo. Así entonces, la autodeterminación informativa es un derecho que faculta a los individuos para que, en su libre desarrollo de la personalidad, decida libremente y bien informado, sobre quién, cómo y para qué, trata sus datos personales, de tal modo que pueda tener el control de los mismos[78].

Respecto a los sujetos, cabe hacer mención que el sujeto universal, sigue considerándose como toda la sociedad en general, es decir, las personas humanas que pueden interactuar con las empresas para realizar transacciones comerciales de bienes y servicios, el sujeto organizado por su parte, siguen siendo las empresas

[78] *Cfr.* Davara Fernández de Marcos, Isabel, *El derecho al olvido en relación con el derecho a la protección de datos personales,* Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, 2014, p. 19, http://www.infodf.org.mx/capacitacion/publicaciones DCCT/ensayo23/23ensayo2014.pdf. Consultado: 15/05/2019.

que ofertan sus productos y servicios en el mercado, sea en establecimientos físicos o en el ciber espacio.

El sujeto cualificado por su parte, requiere especial atención en relación a este derecho, pues derivado de las leyes y de acuerdo a los requerimientos que supone el tratamiento de datos personales en entornos tecnológicos, y más aún en sistemas de cómputo en la nube, hace necesario que el sujeto cualificado cuente con conocimientos de derecho, especialmente en la rama de los derechos humanos, además de tener un alto dominio de las tecnologías que convergen con los datos personales, tales como *Big Data*, inteligencia artificial, cómputo en la nube, así como de los protocolos de comunicación, seguridad de la información, análisis y gestión de riesgos de la información y auditoria de seguridad de la información.

Lo anterior toma relevancia debido a que, en el proceso de comercialización por parte de las empresas, estas deben hacer uso de la tecnología, pero, al usarla para el tratamiento de información, deben tener en cuenta que existe la posibilidad de vulnerar los derechos humanos. A la luz del derecho a la protección de datos personales, una manera de vulnerar este derecho es mediante el uso desproporcionado de la tecnología, sea para investigar –vulnerando la privacidad e intimidad– o para difundir información de la esfera privada o íntima de las personas.

Por ello, para fundamentar los requisitos que se han descrito anteriormente, respecto a, quien se le debe considerar como sujeto cualificado; es de interés lo que ha establecido la sección cuatro del *Reglamento General de Protección de Datos del Consejo de Europa* como funciones del Delegado de Protección de Datos, a quien se le han designado las funciones de:

> 1. El delegado de protección de datos tendrá como mínimo las siguientes funciones: a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;
>
> b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;

> c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;
> d) cooperar con la autoridad de control;
> e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto.
> 2. El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento[79].

Por su parte, el Grupo de Trabajo sobre Protección de Datos del Artículo 29, ha creado las *"Directrices sobre los delegados de protección de datos (DPD)"*[80]*,* donde se establece, respecto a las cualidades del Delegado de Protección de Datos, que este debe tener conocimientos de la organización, de normas y procedimientos administrativos, de sistemas de información y de las necesidades de seguridad y de protección de los datos personales.

En relación a esto, la Agencia Española de Protección de Datos ha diseñado el esquema de certificación[81] para el Delegado de Protección de Datos, en donde se han plasmado todos los requisitos, habilidades y aptitudes que deben contemplarse en los delegados de protección de datos. En torno a ello, podemos decir entonces que las características que hemos señalado como requisito para considerar al sujeto cualificado del derecho a la protección de datos personales, cumplen con lo que se ha establecido en la normativa europea y por la Agencia Española.

Más adelante se analizarán con mayor profundidad el *Reglamento General de Protección de Datos del Consejo de Europa* así como del convenio 108 del Consejo de Europa, con la intención de hacer una comparativa con la legislación mexicana, y sobre dicho análisis reconocer las fortalezas y debilidades de esta legislación.

---

[79] Diario Oficial de la Unión Europea, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo,* 27 de abril de 2016, art. 39, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679. Consultado: 20/11/2019.

[80] *Cfr.* WP, *Directrices sobre los delegados de protección de datos (DPD),* 13 de diciembre de 2016, pp. 12–13, https://www.aepd.es/media/criterios/wp243rev01-es.pdf. Consultado: 20/11/2019.

[81] *Cfr.* Agencia Española de Protección de Datos, *Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos (Esquema AEPD-DPD)*, 13 de junio 2018, https://www.aepd.es/reglamento/cumplimiento/common/esquema-aepd-dpd.pdf. Consultado: 18/11/2019.

*2.3.2. Nuevas tecnologías como factor de origen y evolución del derecho a la protección de datos personales*

Si bien es cierto que la tecnología ha venido evolucionando desde el año 1946 con la creación de la ENIAC y la UNIVAC, hasta llegar a las computadoras modernas de la actualidad, esto representó un peligro para los derechos humanos a partir de la llegada del *Internet* en el año 1969. Mediante el uso de esta tecnología, los derechos humanos relativos a la privacidad de las personas se han visto amenazados, porque el *Internet* supone un nuevo paradigma para transferir información de un lugar a otro en tan solo unos segundos.

Esto que en principio ha maravillado a la sociedad, también representó un gran reto para los derechos humanos y en especial para los juristas de la época, ya que, al transferir informaciones de esta forma, se pierde el control de quién tiene esos datos. Esto comenzó a derivar en la comisión de delitos que se cometían a partir de la intersección de esa información; sea mediante métodos tecnológicos (hacking) o mediante la adquisición pasiva de los mismos (recolección silenciosa).

Sin embargo, pese a las complicaciones que esto ha traído en cuestión de derechos humanos, la aceptación de la tecnología en la sociedad ha sido tal, que hoy en día es impensable un mundo sin tecnología, con la cual nos relacionamos en sociedad y realizamos un sinnúmero de actividades haciendo uso de dichas tecnologías, incluso decidimos poner en riesgo nuestra privacidad para poder seguir utilizando las nuevas tecnologías que cada vez son más invasivas.

Retomando lo que menciona Mónica Arenas Ramiro[82], ella manifiesta que el avance tecnológico y el uso de *Internet*, han traído una serie de acontecimientos que han dado lugar a la generación de ciudadanos informatizados, que se caracterizan por vivir conectados a *Internet* para realizar diversas actividades.

A este fenómeno de la implementación de las tecnologías para el desarrollo de las actividades cotidianas, se le ha denominado como la sociedad de la información, lo que ha dado como resultado la necesidad del reconocimiento de nuevos derechos

[82] Arenas Ramiro, Mónica, "El Reconocimiento de un Nuevo Derecho en el Ordenamiento Jurídico Español: El Derecho Fundamental a la Protección de Datos Personales", en Pérez Pintor, Héctor (coord.), *El Iusinformativismo en España y México,* Morelia, Michoacán, México: División de Estudios de Posgrado de la Facultad de Derecho y Ciencias Sociales UMSNH, 2009, p. 150.

que antes no se conocían, como el derecho a la intimidad para controlar el uso que terceras personas puedan hacer con nuestra información personal, entre otros derechos relacionados con la privacidad.

Por su parte, Ana Garriga Domínguez menciona que el derecho a la protección de datos personales es un derecho complejo, puesto que:

> […] el derecho a la protección de datos personales es, sobre todo, un derecho con un contenido predominantemente positivo. Éste se concreta en un conjunto de instrumentos que garantizan a las personas la posibilidad de ejercer un control efectivo sobre el uso y destino de sus datos, permitiéndole saber, quién, dónde, cuándo y para qué ha obtenido y registrado informaciones que les conciernen. […][83]

La llegada del *Internet* supone una mayor libertad de expresión, ya que permite que todas las personas podamos ejercer las facultades que el derecho a la información nos garantiza para poder investigar, recibir y difundir información de toda índole, sin limitación de fronteras. Sin embargo, al mismo tiempo, con la proliferación de los sistemas que operan en línea y el creciente uso de las redes sociales, se ha visto amenazada la privacidad e intimidad de las personas.

Esto no significa que dichas tecnologías sean malas, sino más bien, la aplicación de esas tecnologías a los procesos cotidianos con los que interactúan las personas, ha dado lugar al tratamiento desproporcionado de datos personales, generando la necesidad de reconocer nuevos derechos que garanticen a los ciudadanos el respeto a su privacidad e intimidad, mediante el establecimiento de deberes y obligaciones para las empresas que recolectan y tratan datos personales.

Así pues, como ya se ha mencionado anteriormente, desde los años 70s se vislumbraba que el uso de las tecnologías de la información suponía una amenaza para la privacidad de las personas por el mal uso de las mismas, lo que generó la necesidad de comenzar a trabajar en la legislación pertinente, para regular el tratamiento de los datos de carácter personal que se almacenan en los dispositivos tecnológicos.

---

[83] Garriga Domínguez, Ana, “El derecho a la protección de datos personales en la jurisprudencia del tribunal constitucional”, *Nuevos retos para la protección de Datos Personales. En la Era del Big Data y de la computación ubicua,* Dykinson, 2015, p. 95.

Derivado de ello, y como medida para limitar el uso de la informática para garantizar la privacidad de las personas, se creó la primera ley sobre tratamiento de datos personales en el año de 1970 en el estado de *Land de Hesse,* en la *República Federal Alemana*.

Posteriormente, en el año 1973, se crea en *Suecia* la que se podría considerar como la primera ley de protección de datos personales en el mundo, y a partir de ello se comienzan a crear otras leyes en torno a la protección de datos personales en otros países.

En 1974 se crea en Estados Unidos la *Privacy Act*[84], siendo estas tres leyes las que originan el reconocimiento del derecho a la protección de datos personales y sobre las cuales se han basado la mayoría de las leyes subsecuentes que se han replicado a lo largo del planeta, bajo la premisa de garantizar la privacidad y la intimidad de las personas frente al uso de las nuevas tecnologías de la información y la proliferación del uso de *Internet*.

Ya hemos dicho que el derecho a la protección de datos personales protege la privacidad e intimidad de las personas, sin embargo, al hablar de privacidad e intimidad nos encontramos con el problema para definir qué es lo privado y qué es lo íntimo de una persona, lo cual, ya hemos diferenciado con anterioridad para poder comprender la importancia del derecho a la protección de los datos personales, para la salvaguarda de los derechos de la personalidad.

Debe entenderse la privacidad como esa esfera de la vida privada en la que convergen datos relacionados a la persona, pero que por su naturaleza son datos que deben circular de manera libre en sistemas informáticos, acción necesaria para el desarrollo comercial y las relaciones personales, con la única limitante que contemplan las leyes para proteger a las personas contra toda intromisión arbitraria de terceros, con la finalidad de proteger el honor, la reputación, la propia imagen y la dignidad.

Por su parte, la intimidad se entiende como un espacio espiritual, íntimo y reservado de las personas, el cual involucra a las familias y tiene especial

---

[84] Internal Revenue Service, *Privacy Act of 1974,* https://www.federalregister.gov/documents/2018/06/11/2018-12462/privacy-act-of-1974

protección, ya que, de ser transgredido, esto podría dar origen a la discriminación y exclusión de círculos sociales, impidiendo de cierta manera el libre desarrollo de la personalidad.

Por lo tanto, el derecho a la protección de datos personales, es un derecho que busca garantizar la protección de ese espacio privado e íntimo de las personas, entendiendo que los datos personales que convergen en la esfera de la privacidad, pueden circular de manera libre bajo ciertos estándares de protección, y con apego a los principios que rigen el tratamiento de los mismos. Esto garantiza que circulen en el mercado global para establecer relaciones comerciales, con sus respectivas excepciones en pro de la seguridad e integridad física de las personas.

Por su parte, todos los datos personales que pueden dar origen a la discriminación o exclusión de los grupos sociales, corresponden a la esfera íntima de las personas, los cuales son conocidos como datos personales sensibles, mismos que gozan de una especial protección por la ley. De tal suerte que las tecnologías no deberían ser usadas para conocer datos sensibles relacionados a las personas, como lo supone el análisis del comportamiento de los usuarios en *Internet.*

Como ya hemos visto, este derecho surge como una necesidad de regular el tratamiento de la información en las tecnologías de la información, que por su naturaleza permite que la información inherente a una persona sea distribuida a nivel mundial con tan solo dar un clic y que derivado de ello, puede verse afectada la privacidad e intimidad y, más aún, el uso desproporcionado de los datos personales puede poner en riesgo, incluso, la seguridad e integridad, así como la vida misma de los propietarios de dichos datos.

### *2.4. Principios, deberes y obligaciones de la protección de los datos personales*

Antes de comenzar a describir cada uno de los principios que rigen la protección de datos personales, es necesario hacer mención de lo que se considera como un principio. Para ello, se presida mencionar que los principios están estrechamente ligados con los valores humanos, es decir se entienden como el inicio de la sana

convivencia social en donde se supone que todas las personas deben tener valores que permitan caminar juntos como sociedad en busca de la felicidad.

Los principios suponen entonces que todas las personas se conducirán de manera correcta sin violentar los derechos de terceros, sin la necesidad de que una norma específica regule la conducta, sino más bien, sean las mismas personas las que se autorregulan con base en sus valores éticos y morales.

Sin embargo, en la actualidad se han perdido ciertos valores humanos, lo que hace necesario que las leyes fijen dichos principios para regular la conducta de los individuos, estableciendo qué está bien y qué está mal, o qué se permite y qué no, en una sociedad.

Desde esta perspectiva podemos definir los principios como un conjunto de valores, creencias, normas, que orientan y regulan la conducta humana en sociedad y que tienen como finalidad garantizar el goce de los derechos de las personas, sin que éstas se vean afectadas en su libre desarrollo de la personalidad por intereses particulares o colectivos.

Así entonces, el derecho a la protección de datos personales se sustenta en ocho principios fundamentales que rigen los deberes y obligaciones de los responsables de la protección de los datos personales, los cuales se describen a continuación.

De la Ley también se deriva el requisito para todos los responsables del tratamiento de los datos personales exhiban un aviso de privacidad, ya sea en formato impreso, digital, sonoro o cualquier otro existente mediante el cual se le informará a los titulares de los datos sobre: qué datos se recolectan, con qué finalidades, con quién los comparte, qué medidas de seguridad existen para garantizar la integridad de los datos personales, el procedimiento para ejercer los derechos ARCO y los medios de contacto con el departamento o encargado de dar respuesta a las solicitudes de derechos ARCO.

*A. Principios de la protección de datos personales*

Los principios planteados en la Ley tienen como objetivo que los responsables tengan una guía sobre los parámetros que deberán cumplir en el proceso del

tratamiento de los datos personales, con ello se garantiza el respeto del derecho la protección de estos datos, a la intimidad e integridad física de las personas.

*1. Principio de licitud:* El primer párrafo del artículo 7 de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, en concordancia con el artículo 10 del *Reglamento de la Ley General de Protección de Datos Personales en Posesión de los Particulares*, –en lo sucesivo "el Reglamento"– obliga al responsable a que el tratamiento de los datos personales se haga conforme a los principios que rigen el tratamiento de los datos personales, con apego a la legislación mexicana y al derecho internacional, así como el acatamiento de los convenios, tratados o directivas en materia de protección de datos personales de los que México sea parte, garantizando de esta manera el respeto a este derecho.

*2. Principio de lealtad:* Fundamentado en los párrafos segundo y tercero del artículo 7 de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, y en relación con el artículo 44 del Reglamento, este principio está vinculado con el de licitud o principio de lealtad y legalidad que obliga al responsable a que los datos recolectados se usen para finalidades lícitas y legales, que no atenten contra su titular ni contra terceros. Este principio supone la expectativa razonable de que los datos recolectados serán tratados de manera lícita, conforme a lo acordado y bajo los términos establecidos en el aviso de privacidad, así como a no recabar datos personales con dolo, mala fe o para beneficios personales. Esto dará a los titulares la confianza para depositar sus datos con el responsable.

*3. Principio de consentimiento:* Este principio encuentra su fundamento en los artículos 8, 9 y 10 de la ya mencionada Ley, así como los artículos del 11 al 22 del Reglamento. Es uno de los principios de mayor importancia, ya que sin el consentimiento, no sería posible tratar de manera lícita los datos personales. La finalidad es que el responsable no trate datos personales sin el consentimiento expreso o tácito del titular y, aun cuando se haya obtenido dicho consentimiento, el titular podrá revocarlo mediante el ejercicio de los derechos ARCO, siempre que no exista relación jurídica contractual que lo impida.

Cabe señalar que el consentimiento podrá ser recolectado en cualquiera de las tres formas que la Ley permite y según el tipo de datos de que se trate. Siendo

requisito el consentimiento tácito para el tratamiento de cualquier tipo de dato personal, con excepción de los datos patrimoniales, financieros y sensibles.

El consentimiento expreso se divide en expreso, y expreso y por escrito, siendo requisito el consentimiento expreso que puede ser de manera verbal, escrita o mediante cualquier otro símbolo que haga suponer la aceptación de los términos del tratamiento por el titular, para el tratamiento de datos financieros o patrimoniales.

Sin embargo, para el tratamiento de datos sensibles, es requisito recolectar el consentimiento expreso y por escrito manifestando la aceptación mediante firma, huella dactilar o cualquier otro mecanismo autorizado por la normativa para autenticar al titular, ya que el tratamiento de los datos sensibles conlleva una responsabilidad mucho más amplia por las consecuencias que el mal uso de los mismos podría ocasionar al titular.

*4. Principio de calidad:* Su fundamento se encuentra en el artículo 11 de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, así como en el artículo 36 el Reglamento. Este principio hace referencia a que los datos que el responsable conserva sobre el titular deben ser correctos, exactos y completos y estar actualizados según sea necesario con respecto a los fines para los cuales se hayan recopilado. El responsable también se obliga a cancelar los datos cuando estos hayan dejado de ser necesarios, así como a eliminar información relativa al incumplimiento de relaciones contractuales que propicien el menoscabo del honor, la honra o la reputación del titular.

El principio de calidad está relacionado con el derecho de cancelación, pues el mismo artículo infiere que, cuando los datos hayan dejado de ser necesarios o así lo solicite el titular, estos sean eliminados conforme al procedimiento establecido en la Ley y el reglamento, con fundamento en los artículos 37, 38 y 39 del Reglamento, los cuales indican de manera somera el plazo de conservación, el procedimiento para la conservación, bloqueo, supresión de los datos, así como la prueba del cumplimiento de los plazos de conservación.

*5. Principio de finalidad:* Se fundamenta en el artículo 12 de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* y en concordancia con los artículos 40, 41, 42 y 43 del Reglamento. Su finalidad es la manifestación

esencial de la protección de la privacidad en relación con el tratamiento de los datos personales, proporciona los elementos necesarios al titular para que decida libremente si proporciona o no sus datos personales al responsable según las finalidades primaria y secundaria para la cual serán recolectados, así como las medidas de seguridad implementadas para garantizar la confidencialidad y seguridad de los datos.

Ello significa que el responsable, además de recolectar los datos para una finalidad primera, la cual debe ser informada de manera clara al titular, también puede usar dicha información para finalidades distintas, mismas que deben ser análogas a la finalidad primaria. El titular, por su parte, tiene la facultad para oponerse al tratamiento de sus datos para dichas finalidades distintas a la finalidad primaria que dio origen al tratamiento de los mismos.

Cabe señalar que, el tratamiento de datos personales en contravención a este principio, puede derivar en una multa contra el responsable, que va de los 200 a los 320,000 días de salario mínimo vigente en el Distrito Federal (ahora Ciudad de México). De tal manera que el responsable no puede cambiar sustancialmente la finalidad original del tratamiento de los datos sin observar lo que se establece en el artículo 12 de la Ley.

*6. Principio de proporcionalidad:* En el artículo 13 de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, y en concordancia con los artículos 45 y 46 del Reglamento, refieren que los datos personales que se recolectan, deben ser proporcionales según lo exija la relación con el titular, y no deberán recolectarse más datos de los que resulten adecuados y relevantes en relación con las finalidades previstas en el aviso de privacidad, de igual manera, supone el esfuerzo razonable del responsable por limitar el uso de los datos sensibles al periodo mínimo e indispensable para el cumplimiento de la finalidad para la cual sean recolectados.

De tal manera que, este principio se sustenta en el criterio de minimización, es decir, el responsable debe recolectar los datos mínimos necesarios para dar cumplimiento a la relación contractual con el titular. Es importante señalar que cuando se refiere a datos personales sensibles, estos deberán ser tratados

conforme a los supuestos establecidos en el artículo 56 del Reglamento y en concordancia con el artículo 9, párrafo dos de la Ley; aunque lo más pertinente es no recolectar este tipo de datos si no son indispensables para el cumplimiento de la relación jurídica existente.

*7. Principio de responsabilidad:* En el artículo 14 de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, así como los artículos del 47 al 55 del Reglamento, especifican que el responsable del tratamiento de los datos personales deberá asegurar el cumplimiento de los principios, debiendo adoptar las medidas pertinentes para su aplicación. Cuando el responsable haya nombrado algún encargado para que a su nombre realice el tratamiento de los datos, seguirá siendo responsable de velar por el cumplimiento de los principios y de la Ley en general, pues las sanciones derivadas del mal uso de los datos personales seguirán siendo aplicables al responsable y no al encargado.

*8. Principio de información:* Los artículos 15, 16, 17, 18 y 20 de la mencionada Ley, y en relación con los artículos del 23 al 35 del Reglamento, son el fundamento del principio que obliga al responsable de los datos personales a poner a disposición del titular el aviso de privacidad mediante el cual se le informa, entre otros aspectos, qué datos personales se recolectan, con qué finalidades, con quién los comparte y con qué medidas de seguridad contarán dichos datos. Así el titular estará en condiciones para ejercer su derecho a la autodeterminación informativa, decidiendo de manera informada si proporciona sus datos personales al responsable.

De igual manera, en relación al artículo 112 del Reglamento, cuando el responsable recolecte datos sin intervención humana, deberá informar este hecho al titular; tal es el caso de las *cookies*[85]*, beacons*[86]*,* teléfonos inteligentes[87], cámaras de videovigilancia (CCTV) o cualquier otra técnica de recolección de información.

---

[85] *Cfr.* Rivera Sanclemente, María del Rosario, *La evolución de las estrategias De marketing en el entorno Digital: implicaciones jurídicas,* [Tesis doctoral], Universidad Carlos III, Madrid, 2015, p. 299. https://e-archivo.uc3m.es/bitstream/handle/10016/22498/rosario_rivera_tesis.pdf.

[86] "Los beacons o balizas son pequeños dispositivos que se pueden montar fácilmente en, por ejemplo, una pared y que se conectan con el móvil del usuario. Frente a otras tecnologías como la NFC ofrece la ventaja de que su alcance llega hasta los 50 metros"". Romero Monserrat", George Alexis, Solución de Marketing Interactivo de Proximidad Basado en Tecnologías de Campo Cercano, Universidad de Cantabria, 3014, pp. 18–19, https://pdfs.semanticscholar.org/023e/8565e73a3b6362a45b14aaee361d8f825cdb.pdf"

[87] *Cfr.* Peirano, Martha, El enemigo…, *Op. Cit.* pp. 97–104.

La violación a este principio puede derivar en la imposición de una sanción económica que va de los 100 a los 160,000 días de salario mínimo vigente en el Distrito Federal (ahora Ciudad de México).

De los mismos principios se derivan deberes y obligaciones que permiten dar cumplimiento a dichos principios de la protección de datos personales, ligando los derechos con los principios, deberes y las obligaciones que la ley establece como acciones mínimas necesarias para garantizar el derecho a la protección de datos personales.

Así entonces, los principios delimitan la responsabilidad derivada del tratamiento de los datos personales para la efectiva protección de la privacidad e intimidad de las personas que han entregado los datos personales, establece la necesidad de adoptad medidas de seguridad administrativas, técnicas y físicas para garantizar la privacidad, integridad y seguridad de los datos personales y supone las sanciones pertinentes en caso de que el responsable no cumpla con lo informado en el aviso de privacidad, los deberes y obligaciones que el tratamiento de datos personales deriva.

*B. Obligaciones*

El responsable estará obligado a cumplir con las disposiciones establecidas en la Ley y su Reglamento. Además, es importante hacer hincapié en que el artículo 19 de la Ley obliga al responsable a que adopte “medidas de seguridad administrativas, técnicas y físicas […], [así como las medidas de seguridad pertinentes para garantizar la confidencialidad, integridad de los datos de los titulares] contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado”[88].

Consecuentemente, el responsable se obliga a actuar de manera lícita, ética y a tratar los datos solo para cumplir con la relación jurídica que exista entre el titular y el responsable, y no deberá utilizar dicha información para beneficio propio, ni para finalidades secundarias que no se hayan dado a conocer al titular de los datos personales mediante el aviso de privacidad.

[88] Ley Federal de Protección de Datos Personales…, *Op. Cit.* p. 6.

Así, la finalidad de las obligaciones relacionadas con cada uno de los principios, es que el titular cuente con la información necesaria para poder decidir sobre su información y a quién se la proporciona, con pleno conocimiento de las finalidades para las que su información es recolectada y con la garantía de que sus datos no serán utilizados en detrimento de su patrimonio, honor, dignidad, reputación o su propia imagen.

*C. Deberes*

Los responsables del tratamiento de los datos personales, al recolectar información de los titulares, deben implementar acciones que permitan garantizar el respeto del derecho a la protección de datos personales. Por lo que, además de cumplir con cada uno de los principios enunciados, es necesario que se cumpla con los deberes de confidencialidad y de seguridad de los mismos.

a. Deber de confidencialidad de los datos personales

El responsable de los datos personales tiene el deber de garantizar que los mismos permanecen en secrecía para terceras personas que no son parte del proceso en el que son tratados; este deber se puede relacionar con el secreto profesional, ya que son datos que se obtienen para cumplir con una finalidad concreta y todo uso fuera de esa finalidad supone una sanción para el responsable.

Por otro lado, el acceso a los sistemas informáticos pone en riesgo toda la información que en ellos se encuentre almacenada, sin distinguir entre información actualizada, información cancelada (oculta) o datos sensibles. De tal manera que el deber de confidencialidad obliga al responsable a vigilar la seguridad de los sistemas informáticos para garantizarla, aun cuando ya no exista relación jurídica entre el titular y el responsable.

En caso de que el responsable haya contratado a un tercero como encargado de los datos personales, debe de cerciorarse de que la información cuenta con las medidas tecnológicas necesarias para garantizar su seguridad, impidiendo que sean tratados por terceros ajenos al responsable o a quienes este haya designado.

Este deber tiene como fundamento el artículo 21 y su objetivo es evitar daños al titular de los datos personales, ya que, de no ser así, cualquier persona podría tener acceso a ellos y, una vez teniendo el conocimiento de donde localizar a una persona, poder realizar algún acto delictivo en su contra. "[…] A tal fin, es conveniente que el responsable adopte e implemente tanto una política de confidencialidad como otras medidas, tales como contratos o cláusulas contractuales a firmar con quienes intervengan en el tratamiento de datos personales" […][89].

También es necesario hacerse las siguientes preguntas para verificar la efectividad de la protección de los datos personales:

> ¿Tiene implementadas medidas para garantizar la confidencialidad de los datos personales que trata; ¿Se asegura de que sus empleados, encargados o terceros guarden confidencialidad respecto de los datos personales a los que tienen acceso? y ¿Prevé sanciones en caso de incumplimiento del deber de confidencialidad?[90]

*b.* Deber de seguridad de los datos personales

En el artículo 19 de la Ley y en concordancia con el principio de responsabilidad, se establece el deber de seguridad, que hace necesaria la implementación de medidas de seguridad administrativas, técnicas y físicas. El artículo 20 deja claro el deber de informar a los titulares de los datos personales cuando exista alguna vulneración que pueda poner en riesgo los derechos patrimoniales o morales de la persona, pues el responsable del tratamiento de los datos personales, mediante este deber, está obligado a implementar mecanismos de seguridad para mantener en secrecía la información; dichas medidas de seguridad deberán responder a las necesidades del análisis de riesgo de los datos, para que el costo de su protección no resulte más costoso que los bienes a proteger.

Para ello es necesario que el responsable realice el análisis correspondiente a los datos personales que son tratados en los sistemas tecnológicos, sea en la nube

---

[89] INAI, *Principios y deberes en materia de Protección de Datos Personales*, México, Espacio de Formación Multimodal, p. 65.

[90] INAI, *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* México, 2016, p. 69, http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

o en entornos locales, y posteriormente, deberá tener en cuenta los parámetros que se ilustran en la figura 2.2.


Figura 2.2. Parámetros para la implementación de seguridad de los datos personales
*Fuente: INAI, Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, p. 70.*

En cuanto a las acciones que el responsable debe adoptar para lograr cumplir con el deber de seguridad de los datos personales, es necesario que se consideren las siguientes:

I. Elaborar un inventario de datos personales y de los sistemas de tratamiento;
II. Determinar las funciones y obligaciones de las personas que traten datos personales;
III. Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales;
IV. Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva;
V. Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales;
VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha;
VII. Llevar a cabo revisiones o auditorías;
VIII. Capacitar al personal que efectúe el tratamiento, y
IX. Realizar un registro de los medios de almacenamiento de los datos personales[91].

Una vez que se haya hecho el análisis principal bajo estas consideraciones, es preciso elaborar el análisis de riesgos que permita obtener un panorama más amplio en cuanto al número de titulares, el riesgo inherente a los tipos de datos personales que son tratados y las posibles afectaciones tanto para los titulares como para la empresa. A partir de ello, se estará en condiciones de implementar los mecanismos necesarios para mitigar los riesgos detectados.

[91] *Ibidem,* p. 71.

Así entonces, es te deber deriva en la obligación de implementar las medidas de seguridad administrativas, técnicas y físicas que contempla la ley en el artículo 19, que tiene como objetivo proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. Esto se desglosa en las siguientes obligaciones:

I. Establecer y mantener medidas de seguridad administrativas, físicas y técnicas;
II. No adoptar medidas de seguridad menores a aquéllas que mantengan para el manejo de su información;
III. Tomar en cuenta el riesgo inherente por tipo de dato personales; las posibles consecuencias para los titulares por una vulneración; la sensibilidad de los datos personales tratados y el desarrollo tecnológico;
IV. Considerar las acciones que establece el artículo 61 del Reglamento de la LFPDPPP para la implementación y mantenimiento de las medidas de seguridad;
V. Actualizar las medidas de seguridad implementadas, cuando así se requiera, según los criterios antes descritos;
VI. Notificar a los titulares las vulneraciones de seguridad que se presenten, con la información y en el momento antes señalados;
VII. Llevar a cabo las acciones correctivas que sean necesarias[92].

Respecto a las medidas de seguridad administrativa, se retoma el concepto del artículo 2 del Reglamento, que refiere que son un "conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, […] así como la concienciación, formación y capacitación del personal, en materia de protección de datos personales"[93].

Por su parte, las medidas de seguridad físicas, se refieren a los mecanismos implementados para mantener la seguridad de la información, impedir el acceso no autorizado a los equipos que almacenan la información, proteger los equipos de cómputo portátil y los dispositivos móviles, y garantizar la eliminación de manera segura de los datos cuando así lo permita la Ley, sea mediante solicitud del titular o porque ya expiró el plazo de conservación de los mismos.

En tanto que, las medidas de seguridad técnicas se definen en el artículo 2 del Reglamento como "Conjunto de actividades, controles o mecanismos con resultado

---

[92] *Ibidem,* p. 73.
[93] Diario Oficial de la Federación, *Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, publicado el 21 de diciembre de 2011.

medible, que se valen de la tecnología para asegurar"[94] que el tratamiento de los datos personales se realiza por personal identificado y autorizado, solo para el cumplimiento de sus funciones, así como acciones necesarias para el desarrollo, adquisición, mantenimiento de sistemas seguros y gestión de las comunicaciones y equipos informáticos.

*2.4.1. El aviso de privacidad y sus tipos*

El aviso de privacidad es la parte primordial del principio de información, ya que es el medio por el cual el responsable de los datos personales informa al titular de los mismos sobre todos los aspectos que la ley establece como parte indispensable para que el titular pueda ejercer su autodeterminación informativa.

El aviso de privacidad es el elemento físico, digital o en cualquier otro medio susceptible de ser transmitido, recibido y entendido por el titular, mediante el cual, el responsable le informa sobre los datos personales que de él se recaban, las finalidades primarias y secundarias, el tiempo de almacenamiento de los mismos; así como los detalles de con quien comparte dichos datos, la seguridad con la que cuentan y el procedimiento para ejercer sus derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO).

Gracias a este documento, mediante el que, el responsable informa al titular sobre el tratamiento que hará de sus datos personales, este último podrá estar en condiciones de ejercer su autodeterminación informativa, es decir, sabiendo que datos recolectan de él y con qué finalidades, podrá decidir libremente a quién y para qué entrega sus datos, o si rechaza dicho tratamiento.

Independientemente de que el titular haya aceptado las condiciones del responsable respecto al tratamiento de sus datos personales, podrá ejercer sus derechos ARCO para tomar decisiones en relación con sus datos, siempre y cuando esas decisiones no se interpongan a la finalidad primaria, la cual debe prevalecer mientras existe relación jurídica derivada de la prestación del servicio entre el titular y el responsable.

---

[94] *Idem.*

Cabe mencionar que mientas existe una relación jurídica que evite que los datos personales sean cancelados o tratados para los fines que se hayan obtenido, el titular solo podrá oponerse al tratamiento para las finalidades secundarias, entendidas como aquellas finalidades que no son necesarias para la prestación del servicio que se haya contratado con el responsable.

Existen tres tipos de avisos de privacidad, los cuales tienen características específicas que los diferencian entre sí y los cuales se utilizan según las condiciones de estación y medio por el cual se dan a conocer:

El *aviso de privacidad integral*, es el aviso de privacidad más completo en el cual se le presenta al usuario toda la información de interés y que le permite ejercer su autodeterminación informativa. En dicho aviso se incluyen de manera clara y detallada los datos que se recolectan, las finalidades para las que se recolectan, las medidas de seguridad implementadas para proteger dichos datos, los mecanismos y procedimientos para ejercer sus derechos ARCO, algunas recomendaciones que aumenten la seguridad de la información, si utiliza algunos mecanismos para la recolección de datos como las *cookies* o alguna otra tecnología y la fecha de actualización del aviso de privacidad.

El *Aviso de privacidad simplificado*, tiene la misma finalidad, pero se utiliza cuando el espacio en el cual se va a dar a conocer al usuario es reducido y no cabría el total del texto que contiene el aviso de privacidad integral, sin embargo, sí da a conocer al usuario los datos que de él se recolecta y debe tener un enlace que redireccione al aviso de privacidad integral.

El *Aviso de privacidad corto,* se utiliza cuando este es dado a conocer a los titulares mediante mensajes de texto en dispositivos móviles o en mensajes de audio, los cuales deben ser cortos para no abrumar al usuario, sin embargo, estos también deben proporcionar el enlace para que el usuario pueda consultar el aviso de privacidad integral y pueda otorgar el consentimiento para el tratamiento de sus datos personales de manera libre a informada.

Este documento que se hace obligatorio dar a conocer por los responsables a los titulares, se considera como el documento clave del respeto del derecho a la

protección de datos personales, ya que de ello depende que el titular pueda ejercer su autodeterminación informativa de manera informada.

Por tanto, no contemplar alguno de los aspectos que exige la ley, vía el aviso de privacidad, la empresa estaría siendo objeto de una sanción por no cumplir con los requerimientos que la ley exige se den a conocer al titular mediante el aviso de privacidad.

Cabe señalar que cuando los titulares hacen uso de algún servicio en línea, mediante alguna plataforma tecnológica en donde deben aceptar los términos del aviso de privacidad, además de cumplir con los requisitos que exige la ley, se debe tener en cuenta que no debe marcarse por default la aceptación de dichos términos, ya que esto implicaría decidir por el titular y quitarle la facultad de decidir libremente si está de acuerdo o no con las finalidades y la forma en la que van a ser tratados sus datos personales. Esto constituye una violación al derecho a la autodeterminación informativa.

### *2.5. Los Derechos de acceso, rectificación, cancelación y oposición*

Ya se han mencionado anteriormente los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO), ahora se dará una breve explicación de cada uno de ellos. Estos derechos facultan a los titulares para poder acceder a sus datos, pedir la rectificación cuando sea necesario, la cancelación cuando así lo permita la ley y la oposición al tratamiento de sus datos cuando estos estén siendo tratados para alguna finalidad secundaria o fuera de lo acordado en el aviso de privacidad.

#### *2.5.1. Derecho de acceso*

Así entonces, el derecho de acceso permite al titular de los datos solicitar a los responsables que le den a conocer qué datos relacionados a su persona conservan, con que finalidades, las medidas de seguridad implementadas e incluso puede solicitar que se le informe si sus datos se han visto comprometidos por algún ataque informático. De esta manera, –sin que se entienda el acceso como un requisito previo– el titular estará en posibilidad de ejercer cualquiera de los otros tres derechos con respecto al tratamiento de su información personal.

A interpretación del artículo 23 de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* así como los artículos 101 y 102 del Reglamento, el acceso permite acceder a los datos que el responsable tiene en su poder, así como conocer el aviso de privacidad, en el cual, como ya se mencionó anteriormente, es el instrumento mediante el cual se dan a conocer al titular las finalidades, los medios para ejercer sus derechos ARCO, si es que sus datos se comparten con alguna otra empresa, así como las medidas de seguridad implementadas.

*2.5.2. Derecho de rectificación*

Por su parte, el derecho de rectificación contemplado en el artículo 24 de la Ley y en los artículos 103 y 104 del Reglamento, facultan al titular para pedir que sus datos sean rectificados, es decir, si se detecta que los datos relacionados a su persona que obran en posesión del responsable son incorrectos, podrá, mediante el ejercicio de este derecho solicitar al responsable su corrección.

Esto aplica en caso de que los datos sean incorrectos o no se encuentren actualizados, por ejemplo, si el titular tiene una cuenta por pagar con un proveedor y dentro del periodo ordinario se cubre dicha deuda, pero posterior a su pago se le realizan llamadas para requerirle dicho pago, es porque la información no se actualizó de manera oportuna, lo cual abre la posibilidad de ejercer este derecho.

Ahora bien, de acuerdo con el principio de calidad establecido en el artículo 11 de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* es conservar solo los datos pertinentes, correctos y actualizados para el cumplimiento de las finalidades que dieron origen al tratamiento. Esto no garantiza que, cuando el responsable comparte la información con un tercero para cuestiones administrativas –como la recuperación de cartera vencida– la información con la que cuenta el tercero se actualizada, en cuyo caso, el titular podrá requerir al responsable la actualización de la información.

*2.5.3. Derecho de cancelación*

Respecto al derecho de cancelación, es la facultad que tienen los titulares de los datos para solicitar al responsable que elimine la información que obre en sus sistemas o expedientes relacionada a su persona, esto claro, cuando la ley así lo permita, pues no se podrá eliminar la información cuando aún sea necesaria para el cumplimiento de alguna obligación contractual entre el titular y el responsable.

En tal sentido, el artículo 25 de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* especifica que, los datos personales previo a su cancelación, deberán ser bloqueados por un periodo "equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en los términos de la Ley aplicable en la materia".

De tal manera que, este derecho solo podrá ser ejercido cuando no haya alguna condición legal que lo impida. Por ejemplo, cuando se contrata un plan de telefonía, el titular de los datos no podrá solicitar la cancelación de sus datos mientras el contrato siga vigente, en cuyo caso, lo más que podría solicitar es el ejercicio del derecho de oposición que se explica a continuación.

Cuando el responsable hubiese transferido los datos a un tercero, este deberá dar a conocer las solicitudes de cancelación, oposición o rectificación, con la intención de que la información que se tenga de las personas sea correcta, actualizada, o en su caso para que no sea usada conforme a algunas de las finalidades secundarias establecidas en el aviso de privacidad.

Respecto al bloqueo de los datos personales previo a su cancelación, el Reglamento especifica en los artículos 107 y 108 que el responsable deberá establecer un plazo de bloqueo con finalidad impedir el tratamiento de los datos personales, con excepción de su almacenamiento y posible acceso, hasta el plazo de prescripción legal o contractual correspondiente. El plazo del bloqueo deberá ser solo mientras se determinan las posibles responsabilidades en relación con el tratamiento, el cual, de acuerdo a la Ley para Regular a la Sociedades de Información Crediticia, sugiere que este plazo sea por 72 meses a efecto de que se le dé un tratamiento igual al establecido en dicha Ley.

*2.5.4. Derecho de oposición*

En lo que concierne al derecho de oposición, es un derecho que faculta a los titulares de los datos oponerse al tratamiento de los mismos, siempre y cuando no exista alguna condición legal que lo impida, cuando la oposición sea con respecto al tratamiento para alguna de las finalidades secundarias establecidas en el aviso de privacidad.

En tal sentido, es importante recordar que, como ya se mencionó, el aviso de privacidad es el instrumento mediante el cual se le informa al titular sobre qué datos se recaban de él, para que finalidades –primarias y secundarias –se utilizarán sus datos, las medidas de seguridad administrativas, físicas y técnicas que se hayan implementado para proteger dichos datos y el procedimiento para ejercer los derechos ARCO.

Así entonces, la misma Ley permite que la información que se recolecta de las personas, pueda ser tratada para una finalidad primaria, la cual debe ser específica y clara, pero también se puede usar esa información para una o más finalidades secundarias, a dichas finalidades secundarías, sí es posible oponerse en cualquier momento, sin que esto signifique que el ejercicio de este derecho afecte la relación contractual entre el titular y el responsable.

En relación a las finalidades secundarias aludidas, lo más común es que las empresas utilicen la información para fines mercadotécnicos y estadísticos, lo cual está permitido por la Ley. No obstante, el derecho de oposición permitirá evitar ser molestados por publicidad o llamadas relacionadas con el tratamiento de sus datos personales.

Es importante señalar que cuando se ejerce el derecho de oposición, el responsable, al igual que en el ejercicio de los derechos mencionados con anterioridad, está obligado a dar aviso al titular sobre la determinación adoptada con respecto a su solicitud, para ello, más adelante se especificarán los plazos establecidos en la Ley.

En relación a la oposición, es importante señalar que en los artículos 110 y 111 del Reglamento, se hace mención de las alternativas con las que cuenta el titular de los datos para el ejercicio de este derecho, pues los responsables pueden gestionar

listas de exclusión de quienes hayan expresado la negativa para el tratamiento de sus datos personales. De la misma manera, existe el Registro Público de Consumidores y Registro Público de Usuarios, previstos en la *Ley Federal de Protección al Consumidor* y el Registro Público de Usuarios previsto en la *Ley de Protección y Defensa al Usuario de Servicios Financieros,* respectivamente, registros que tienen como finalidad la protección de este derecho.

No obstante, cabe señalar que, tanto los principios como los derechos ARCO, encuentran sus excepciones en el artículo 4 de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* los cuales tienen como finalidad la "protección de la seguridad nacional, el orden, la seguridad y la salud públicos, así como los derechos de terceros"[95].

*A. El ejercicio de los derechos ARCO*

El ejercicio de los derechos antes señalados se llevará a cabo ante los responsables, a iniciativa y voluntad del titular de los datos personales o su representante legal cuando así lo considere necesario. El procedimiento se realizará conforme a lo establecido en los artículos del 28 al 35 de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* en este apartado cabe destacar que, de acuerdo al artículo 29, todas las solicitudes de derechos ARCO deberán ser acompañadas de los siguientes documentos:

> I. El nombre del titular y domicilio u otro medio para comunicarle la respuesta a su solicitud; II. Los documentos que acrediten la identidad o, en su caso, la representación legal del titular; III. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados, y IV. Cualquier otro elemento o documento que facilite la localización de los datos personales[96].

Mientras que el artículo 34 menciona que las solicitudes de tales derechos, podrán ser negadas en los casos de:

---

[95] Ley Federal de Protección de Datos Personales…, *Op. Cit.* p. 3.
[96] Ley Federal de Protección de Datos Personales…, *Op. Cit.* p. 7.

> I. Cuando el solicitante no sea el titular de los datos personales, o el representante legal no esté debidamente acreditado para ello; II. Cuando en su base de datos, no se encuentren los datos personales del solicitante; III. Cuando se lesionen los derechos de un tercero; IV. Cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos, y V. Cuando la rectificación, cancelación u oposición haya sido previamente realizada.
>
> La negativa a que se refiere este artículo podrá ser parcial en cuyo caso el responsable efectuará el acceso, rectificación, cancelación u oposición requerida por el titular[97].

Los plazos en los que el responsable deberá dar respuesta a las solicitudes de derechos ARCO es de 20 días hábiles después de recibida la solicitud, en dicha respuesta le indicará la disposición adoptada, en caso de que la declare procedente, el responsable deberá llevar a cabo las acciones que cumplan con la disposición adoptada en un plazo máximo de 15 días hábiles.

En caso de que la solicitud no cumpla con lo establecido en el artículo 28 de la Ley, el responsable podrá emitir un escrito denominado “prevención”, mismo que deberá comunicar al titular en un plazo máximo de 5 días hábiles contados a partir del día siguiente de la recepción de la solicitud, en él se le debe especificar la información faltante. El titular tendrá 10 días hábiles a partir de la recepción de la “prevención” para solventar la documentación faltante, de lo contrario se entenderá como no presentada la solicitud.

*B. Del Procedimiento para la protección de derechos ante el INAI*

La protección de los derechos es un procedimiento distinto al procedimiento del ejercicio de los derechos ARCO, pues el ejercicio se lleva a cabo ente los responsables que tratan los datos personales, mientras que la protección de los derechos se lleva a cabo ante el órgano garante de dichos derechos –el INAI–, que tiene por función la verificación del cumplimiento de la Ley; el procedimiento se encuentra establecido en los artículos del 45 al 58 de la Ley.

Así entonces, el Procedimiento de Protección de Derechos (PPD) se inicia a solicitud del titular y deriva de la respuesta del responsable respecto al ejercicio de alguno de los derechos ARCO por el titular. La acción que da inicio a este

[97] *Ibidem.* p. 8

procedimiento se conoce como queja, ya que su motivación se origina por la inconformidad de la respuesta, por la negativa de acceso, la negativa a efectuar las rectificaciones o cancelaciones solicitadas, o cuando el responsable siga haciendo uso de los datos para finalidades a las que el titular se haya opuesto anteriormente, o cuando no se dé respuesta a la solicitud del titular.

El área responsable del PPD es la Dirección General de Protección de Derechos y Sanción (DGPDS) en el INAI. Respecto a los plazos para este trámite, el titular tendrá 15 días hábiles a partir de la recepción de la respuesta para interponer su queja ante el INAI; en caso de que la queja sea por omisión a la solicitud, la queja se debe interponer dentro de los 15 días hábiles siguientes al periodo de 20 días con los que cuenta el responsable para dar respuesta a las solicitudes.

Los requisitos para presentar una solicitud de protección de derechos ante el INAI son:

> •El nombre del titular y, en su caso, el de su representante legal, así como del tercero interesado, si lo hay; •El nombre y domicilio del responsable ante el cual se presentó la solicitud de ejercicio de derechos ARCO; •El domicilio para oír y recibir notificaciones; •La fecha en que se dio a conocer al titular la respuesta del responsable, salvo que el procedimiento inicie por falta de respuesta; •Los actos que motivan su solicitud de protección de derechos (describir el motivo de la inconformidad con la respuesta o si ésta se debe por falta de respuesta); •La solicitud de ejercicio de derechos ARCO, así como la respuesta emitida a la misma, en caso de que ésta exista, y •En caso de falta de respuesta, el acuse de recepción de la solicitud de ejercicio de derechos ARCO por parte del responsable. Si el titular no cuenta con este acuse porque el responsable se negó a recibir su solicitud o porque no lo emitió, se deberá informar sobre ese hecho al INAI en la solicitud de protección de derechos[98].

Los medios por los cuales se puede presentar una solicitud de protección de derechos son: de manera presencial en las oficinas del INAI, mediante correo certificado con acuse de recibo, o si se cuenta con firma electrónica se puede presentar en el https://www.datospersonales.org.mx.

Respecto al procedimiento, una vez presentada la solicitud se verificará que cumpla con los requisitos establecidos en el artículo 46 de la Ley, en caso de que

[98] INAI. *Guía para Titulares de los datos personales, Volumen 4: Procedimientos de datos personales ante el INAI.* http://inicio.inai.org.mx/Guias/Guia%20Titulares-04_PDF.pdf, pp. 7–8.

no cumpla con todos los requisitos, el INAI hará la prevención al titular dentro de los 20 días hábiles siguientes a la recepción, para que este a su vez subsane la documentación faltante en un plazo de 5 días hábiles contados a partir de la prevención, en caso de no presentar la documentación, se tendrá por no presentada la solicitud.

Una vez admitida la solicitud, el INAI pedirá al responsable que manifieste lo que a su derecho convenga, así como las pruebas que considere convenientes. Los plazos para ello son, 10 días hábiles cuando se trata de un procedimiento iniciado por falta de respuesta, y de 15 días para los procedimientos iniciados por inconformidad de la respuesta.

No obstante, el INAI en cualquier momento puede llamar a las partes a conciliación, si la conciliación es exitosa, concluirá el procedimiento, buscando siempre garantizar el derecho del titular. Si la conciliación no se lleva a cabo, se deben desahogar las pruebas y se otorga un plazo de 5 días hábiles para que las partes presenten los alegatos y pruebas para poder proceder al cierre de la instrucción, que tiene por objeto que las partes expongan su versión para adoptar la determinación de manera más objetiva.

La resolución del INAI deberá emitirse en un plazo no mayor a 50 días después de presentada la solicitud, y este plazo podrá ampliarse por un periodo igual siempre y cuando exista causa justificada y previa notificación a las partes. La resolución puede ser en los siguientes sentidos: sobreseída o desechada, confirmada, revocada o modificada.

En caso de que se resuelva a favor del titular, el responsable tiene 10 días hábiles para adoptar las disposiciones de la resolución, y cuenta con otros 10 días hábiles para dar a conocer por escrito el cumplimiento al INAI. No obstante, las resoluciones del INAI pueden ser impugnadas mediante juicio de nulidad ante el Tribunal Federal de Justicia Administrativa dentro de los 30 días hábiles posteriores a la resolución, en cuyo caso podrá ser revocada o confirmada dicha resolución.

*2.6. De las sanciones de la Ley*

El Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI), es el órgano garante para la verificación del cumplimiento de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* de tal manera que, en la misma Ley se le otorgan las facultades para la imposición de sanciones a los sujetos regulados cuando así lo amerite la actuación de los mismos, en relación al mal uso de los datos o la violación de los principios que rigen su tratamiento.

En tal sentido, el capítulo IX, relativo al procedimiento de imposición de sanciones, en el artículo 61 se menciona que, "si con motivo del desahogo del procedimiento de protección de derechos o del procedimiento de verificación que realice el Instituto, éste tuviera conocimiento de un presunto incumplimiento de alguno de los principios o disposiciones de esta Ley, iniciará el procedimiento a que se refiere este Capítulo, a efecto de determinar la sanción que corresponda"[99].

De lo anterior se infiere que, entre las atribuciones del INAI, se encuentra la facultad para realizar –de oficio– verificaciones de cumplimiento a la Ley por las empresas, de las cuales podrían derivar sanciones en caso de incumplimiento a los principios contenidos en la Ley y demás disposiciones de la misma. Con respecto a las verificaciones de oficio, estas se inician cuando se da el incumplimiento a resoluciones dictadas por el INAI o a petición de parte[100], además también tiene la facultad para iniciar procedimientos de oficio en casos de interés público que se den a conocer por cualquier medio y donde se suponga la afectación de buena parte de la sociedad.

El Reglamento de la Ley dedica el capítulo IX a las verificaciones realizadas por el INAI, y en dicho apartado se describe el procedimiento de la actuación, el cual puede concluir en el establecimiento de medidas que se deben adoptar en un periodo de tiempo determinado, en el inicio del procedimiento de imposición de sanciones[101].

---

[99] Ley Federal de Protección de Datos… *Op. Cit.* Artículo 61, p. 15.
[100] *Cfr. Ibidem.* Artículo 59, p. 14.
[101] *Cfr.* Reglamento de la Ley de Protección de Datos… *Op. Cit.* p. 34.

Cabe señalar que en el artículo 138 del *Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* se establece la posibilidad de proceder "en contra de la resolución al procedimiento de verificación, se podrá interponer el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa"[102]. Esto da a entender que las resoluciones del INAI no son definitivas y que aún existe este recurso ates de resultar acreedores como responsables a una sanción administrativa o a una pena de prisión.

Si como resultado de los procedimientos de desahogo de protección de derechos o verificaciones, se tiene conocimiento de alguna violación de los principios rectores del tratamiento de los datos personales o de las disposiciones de la Ley, se iniciará el procedimiento de imposición de sanciones, las cuales consisten en multas o penas de prisión, esto dependiendo de la gravedad y de si el tratamiento se considera como una infracción o un delito por el responsable.

Respecto a las multas por infracciones, el artículo 64 de la Ley refiere que estas irán de los 100 a los 160,000 días de salario mínimo vigente en el Distrito Federal –Ahora Ciudad de México–, a las que los responsables se pueden hacer acreedores por "actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales, [así como por] no cumplir con el apercibimiento a que se refiere la fracción I del artículo 64"[103].

En relación a lo anterior, parece ser que el INAI no se ha especializado en la resolución de casos en los que intervenga la tecnología, como se mencionó con anterioridad, en el caso contra Lex Abogados Digitales S.A. de C.V.[104], la resolución contiene elementos de notoria dolía del responsable y, aun así, el órgano garante dio el fallo a favor del responsable por no poder comprobar los dichos del titular que reclamó la protección de sus derechos, que bien, el desahogo del procedimiento con la intervención de un perito en informática forense, hubiese logrado constatar las pruebas del titular y la actuación dolosa por parte del responsable.

En segundo lugar, se encuentran las multas por "incumplir el deber de confidencialidad establecido en el artículo 21 [… y por] Crear bases de datos en

[102] *Idem,* Artículo 138, p. 34.
[103] *Idem,* Artículo 64, Fracción I, p. 17.
[104] *Cfr.* INAI, Expediente PPD.02.13/16…, *Op. Cit.*

contravención a lo dispuesto por el artículo 9, segundo párrafo de esta Ley"[105]. En cuanto a las multas establecidas en este apartado, se determina que sean entre 200 y 320,000 días de salario mínimo en el Distrito Federal.

De igual manera, en la fracción IV del artículo 64, se establece que cuando se reincida en las infracciones de la Ley, las multas podrán incrementar en un rango de 100 a 320,000 días de salario mínimo y cuando se trata de datos personales sensibles, estas podrían aumentar hasta en dos veces más. Traducido en pesos y a manera de ejemplificar los montos derivados de las infracciones a la ley, se presenta la tabla 2.1, que muestra los montos mínimos y máximos a los que se puede hacer acreedor un responsable si no se tiene el cuidado necesario respecto al tratamiento de los datos de sus clientes.

| | Multas por actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales y/o no cumplir con el apercibimiento a que se refiere la fracción I del artículo 64. | | | | Multas por no cumplir con el apercibimiento a que se refiere la fracción I del artículo 64 y/o rear bases de datos en contravención a lo dispuesto por el artículo 9, segundo párrafo de esta Ley. | | | |
|---|---|---|---|---|---|---|---|---|
| Días | De | 100 | a | 160,000 | De | 200 | a | 320,000 |
| Pesos | De | $ 12,322.00 | a | $19,715,200.00 | De | $ 24,644.00 | a | $ 39,430,400.00 |
| En casos de reincidencia podría incrementarse las multas en una suma que irá de los 100 a los 320,000 días de salario mínimo vigente, según lo establecido en el artículo 64 fracción IV de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, lo que daría una suma como la que se muestra a continuación. | | | | | | | | |
| Días | De | 200 | a | 320,000 | De | 400 | a | 640,000 |
| Pesos | De | $ 24,644.00 | a | $39,430,400.00 | De | $ 49,288.00 | a | $ 78,860,800.00 |
| En caso de tratarse de datos sensibles, las multas podrían incrementarse hasta por dos veces, según lo establecido en la fracción IV del artículo 64, dando como resultado cantidades como las que se muestran a continuación. | | | | | | | | |
| NOTA: Se aplica en relación a los establecido en el artículo 9 de la Ley, lo cual significa que en este apartado no aplica este tipo de imposición de multas. | | Días | De | 600 | a | 960,000 | | |
| | | Pesos | De | $ 73,932.00 | a | $118,291,200.00 | | |

Tabla 2.1. Monto de las multas por infracciones a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Salario mínimo vigente en la Ciudad de México.
*Fuente: Elaboración propia*

[105] Ley Federal de Protección de Datos… *Op. Cit.* Artículo 64, Fracción III, p. 17.

Respecto a las multas señaladas en la tabla anterior, son tomadas acorde a lo que establece la Ley en el artículo 64. No obstante, en dicho artículo refiere el salario vigente en el Distrito Federal, hoy Ciudad de México, y debido a que la Ley no ha sufrido reforma alguna para subsanar esta variante, la nueva Constitución Política de la Ciudad de México y desaparición de la figura jurídica del Distrito Federal, podría dejar sin efecto los montos establecidos en este artículo, dando lugar a que actualmente se tome en cuenta la Unidad de Medida y Actualización (UMA), en cuyo caso, las multas quedarían como se muestra en la tabla 2.2.

Cabe señalar en este apartado que, las sanciones que se determinan en las resoluciones del INAI, son ejecutadas por el Servicios de Administración Tributaria (SAT), por lo que no ingresa a los activos del INAI, ni tampoco se pretende con ello reparar los daños y perjuicios de los titulares, por lo que, si así lo deciden, podrán iniciar procedimiento de acuerdo a las leyes aplicables para demandar la reparación del daño ocasionado por el mal uso de sus datos personales.

| | Multas por actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales y/o no cumplir con el apercibimiento a que se refiere la fracción I del artículo 64. | | | | Multas por no cumplir con el apercibimiento a que se refiere la fracción I del artículo 64 y/o rear bases de datos en contravención a lo dispuesto por el artículo 9, segundo párrafo de esta Ley. | | | |
|---|---|---|---|---|---|---|---|---|
| Días | De | 100 | a | 160,000 | De | 200 | a | 320,000 |
| Pesos | De | $ 8,688.00 | a | $13,900,800.00 | De | $ 17,376.00 | a | $ 27,801,600.00 |
| En casos de reincidencia podría incrementarse las multas en una suma que irá de los 100 a los 320,000 días de salario mínimo vigente, según lo establecido en el artículo 64 fracción IV de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, lo que daría una suma como la que se muestra a continuación. | | | | | | | | |
| Días | De | 200 | a | 320,000 | De | 400 | a | 640,000 |
| Pesos | De | $ 17,376.00 | a | $27,801,600.00 | De | $ 34,752.00 | a | $ 55,603,200.00 |
| En caso de tratarse de datos sensibles, las multas podrían incrementarse hasta por dos veces, según lo establecido en la fracción IV del artículo 64, dando como resultado cantidades como las que se muestran a continuación. | | | | | | | | |
| NOTA: Se aplica en relación a lo establecido en el artículo 9 de la Ley, lo cual significa que en este apartado no aplica este tipo de imposición de multas. | | | | Días | De | 600 | a | 960,000 |
| | | | | Pesos | De | $ 52,128.00 | a | $ 83,404,800.00 |

Tabla 2.2. Monto de las multas por infracciones a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Salario mínimo vigente en la Ciudad de México.

*Fuente: Elaboración propia*

Respecto a las penas de prisión por el tratamiento ilícito de los datos personales, lo cual se configura como un delito al tenor de lo establecido en la Ley, en el capítulo XI, relativo a los delitos en materia del tratamiento indebido de datos personales, en el artículo 67 establece que "se impondrán de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia"[106].

Por su parte, el artículo 68 establece que "se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos"[107]. Al respecto, podríamos considerar las aplicaciones que se distribuyen en redes sociales que prometen adivinar el futuro o cualquier otra cosa, las cuales, si se revisa el aviso de privacidad, de cierta manera están informando sobre un supuesto tratamiento, el cual no se puede comprobar, y que en muchos de los casos dicha información se recolecta de manera engañosa con fines lucrativos para el poseedor de los mismos.

En relación a los datos sensibles refiere el artículo 69 que las penas se duplicaran, dando como resultado la tabla 2.3 que se muestra a continuación, donde se muestran las penas de prisión por incumpla lo establecido en la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares.*

| Se impondrán de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia. | | | | Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos. | | | |
|---|---|---|---|---|---|---|---|
| De | 3 meses | a | 3 años | De | 6 meses | a | 5 años |
| Tratándose de datos personales sensibles, las penas a que se refiere este Capítulo se duplicarán. | | | | | | | |
| De | 6 meses | a | 6 años | De | 1 año | a | 10 años |

Tabla 2.3. Penas de prisión por el delito en de tratamiento indebido de datos personales.
*Fuente: Elaboración propia*

[106] *Ibidem,* Artículo 67, p. 17.
[107] *Idem.*

*2.7. El derecho al olvido en relación con el derecho de cancelación*

El más reciente derecho que se ha tratado de integrar a la legislación en torno al tratamiento de los datos personales, es el derecho al olvido, el cual se ha planteado como un derecho de los individuos para pedir que desaparezca de *Internet* aquella información relacionada a su persona, que podría dañar el honor, la reputación o su imagen.

Aunque la intención en este apartado no es debatir si éste debe ser un derecho distinto a los ya reconocidos en la Ley, o si debería encajarse en el derecho a la cancelación. Más bien, la intención es dejar abierto el debate para un análisis más profundo respecto al derecho al olvido y el derecho de cancelación, pues como veremos en seguida, parece que hay una fuerte identidad entre ambos derechos.

Lo anterior en virtud de que, el derecho al olvido tiene lógica si lo vemos desde el punto de vista de la responsabilidad del tratamiento, pues esta responsabilidad es para quien trata los datos personales, mientras que los buscadores, contra quien se ejerce el derecho al olvido, no son los responsables de dicho tratamiento[108], como buscadores, solo indexan información que localizan en servidores de la red de *Internet*, sin que ello signifique que tengan la facultad de eliminarla para que ya no aparezca en *Internet.*

Esto, no exime a los buscadores de la responsabilidad por la recolección desproporcionada de datos personales y el uso para finalidades diversas que podría, *per se,* resultar violatorio al derecho a la protección de datos personales, pero que no está relacionada con la indexación de información en posesión de terceros, pues en este caso, solo es el medio idóneo para la libertad de expresión.

En tal sentido, el motor de búsqueda es el medio idóneo para ejercer las facultades de investigar, recibir y difundir información, la cual alguien difunde para que otros la puedan recibir, aunque el buscador por su parte, pueda negociar con la información que recolecta de los usuarios que usan *Internet,* lo que debe entenderse

---

[108] *Cfr.* Vilasau Solana, Mónica, "El caso Google Spain: la afirmación del buscador como responsable del tratamiento y el reconocimiento del derecho al olvido (análisis de la STJUE de 13 de mayo de 2014)", *Revista de los Estudios de Derecho y Ciencia Política,* Núm. 18, junio 2014, p. 21, http://openaccess.uoc.edu/webapps/o2/bitstream/10609/93657/1/CasoGoogleSpain.pdf. Consultado: 20/08/2019.

como actividades distintas y no análogas a la responsabilidad del tratamiento de la información difundida por un tercero.

Así entonces, el derecho al olvido se ha ejercicio ante las empresas propietarias de los motores de búsqueda, lo cual significa que, para que sea efectivo, tendría que hacerse el mismo procedimiento ante cada una de las empresas propietarias de motores de búsqueda, de lo contrario, solo tendría efecto parcial, pues al cambiar de buscador, la información podría ser nuevamente visible en *Internet.*

Esto parece lógico, porque como ya se mencionó, la empresa propietaria del motor de búsqueda no es la responsable del tratamiento ni la poseedora de la información que se intenta ocultar o eliminar de *Internet.* En ese sentido, al no poder eliminar dicha información, solo puede indicar a su algoritmo de búsqueda que no muestre la información referida.

Sin embargo, parece que este derecho no debería verse como un nuevo derecho, ni tampoco acuñarse un nuevo término para ejercer un derecho que resulta compatible con el derecho de cancelación; tampoco debería ejercerse contra los propietarios de los motores de búsqueda, sino, con aquellos responsables del tratamiento de la información.

En tal sentido, podría existir una reforma a la Ley para que, dentro del derecho a la cancelación, exista una condición para que las empresas propietarias de los motores de búsqueda, cooperen con las autoridades en la localización de los responsables del tratamiento de los datos y así poder ejercer este derecho de cancelación ante el verdadero responsable para que la información que se intenta desaparecer de *Internet* sea efectiva. Por su parte, la empresa del buscador, una vez concretado el procedimiento de cancelación ante el responsable, podría cooperar para eliminar aquellas copias que hayan podido ser almacenada en otros servidores de manera ilícita.

En conclusión, el derecho al olvido no debería contemplarse como un nuevo derecho, pues en realidad como se ha planteado, el ejercicio de este derecho resulta contrario a la libertad de expresión, por ello, parece que el procedimiento más adecuado debería ser acorde al derecho de cancelación, lo cual se puede lograr con una reforma a la Ley, para que los buscadores intervengan solo en la

localización del responsable, cuando esto sea complicado de lograr por las características que presenta la tecnología *per se,* no así, para pedir que estos eliminen u olviden la existencia de la información, pues resulta ilusorio pensar que exista el derecho al olvido en las personas, mucho menos existirá en las tecnologías que trabajan con algoritmos matemáticos y muestran los resultados que concuerden mínimamente con la solicitud de los usuarios.

### *2.8. Reflexiones finales*

A manera de conclusiones del capítulo, en relación a lo que refiere el derecho de la información, se puede decir que el fenómeno informativo en la sociedad de la información está inmerso en la misma sociedad, pues en la actualidad no podemos concebir una sociedad sin todos los medios de comunicación con los que contamos.

Sin embargo, esto también hace necesario que existan normas jurídicas que regulen las relaciones entre particulares y entre el Estado y particulares en torno a la comunicación de información, teniendo como principal objetivo la protección de la información que se ha llegado a concebir como un patrimonio de las personas en la sociedad de la información.

Consecuentemente, en esta sociedad, movida en gran parte por la información y sus derivados, es de suma importancia tener en cuenta que el derecho a la información nos da la facultad como personas para poder investigar, recibir y difundir información, la cual, gracias a las tecnologías, podemos difundir en tan solo unos segundos en el mundo entero.

Por ende, el derecho a la información contempla las facultades, los derechos y las obligaciones que tenemos como sociedad para con la misma sociedad, así como las del Estado para con la sociedad, garantizando al menos en mínima medida que exista la circulación de información sobre la cual se basa gran parte de las decisiones de las personas para encaminar las acciones futuras.

Sin embargo, el derecho a la información no es un derecho absoluto que otorgue la facultad para difundir todo tipo de información de la que nos podamos allegar, pues una de las excepciones es el derecho a la protección de datos personales, el

cual genera también derechos para los ciudadanos y obligaciones para el Estado respecto a la garantía de este derecho.

Dicho derecho también supone sanciones cuando el método utilizado para allegarnos de los datos personales sea ilegal, pues al no contar con el consentimiento, sea tácito o expreso de su titular, estaremos impedidos para poder recolectar y almacenar dicha información y de hacerlo, quien resulte ser el responsable de dicho tratamiento, será sancionado acorde a lo establecido en la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* o en su caso los sujetos obligados acorde a la *Ley Federal de Protección de Datos Personales en Posesión de los Sujetos Obligados.*

Así entonces, retomando la doctrina de José María Desantes Guanter, en lo referente a la identificación de los sujetos, universal, cualificado y organizado para el tema en lo relativo al derecho a la protección de datos personales, se pueden identificar estos tres sujetos de acuerdo al rol que cada uno asume en torno a dicho derecho, como se describe a continuación:

Sujeto universal. Para este caso, el sujeto universal se identifica como todas las personas titulares de datos personales que, en algún momento han proporcionado o proporcionarán en el futuro dichos datos a alguna empresa para la celebración de algún contrato comercial, la prestación de algún servicio o para la compraventa de algún producto. Son al mismo tiempo titulares de derechos como propietarios de los datos que le están entregando a la empresa –particular– y por ende, el Estado a través de su órgano garante, deberá asegurar la salvaguarda de este derecho, permitiendo que exista libertad comercial, pero con pleno respeto a los derechos humanos de las personas.

En lo referente a las empresas particulares, el órgano garante encargado de vigilar el cumplimiento de la Ley en materia de protección de datos personales en las relaciones entre comerciantes y las personas es el INAI, ante el cual los ciudadanos que consideren que se les ha violentado su derecho, podrán interponer un recurso de revisión, a fin de que se le dé el seguimiento hasta llegar a una resolución que pruebe dicho supuesto o determine lo contrario.

En ese tenor, los derechos que el sujeto universal podrá ejercer en torno al derecho a la protección de datos personales, son los derechos de acceso, rectificación, cancelación y oposición, los que, en su conjunto, conforman las facultades de los titulares para lograr un desarrollo pleno de la personalidad sin limitantes para interactuar con las empresas, entorno que más adelante se denomina como la economía digital.

Sujeto cualificado. Por lo que respecta al sujeto cualificado para este caso, se puede entender como aquella persona con los conocimientos mínimos necesarios para poder garantizar la salvaguarda de los datos personales en el entorno tecnológico, así como salvaguardar el derecho de los titulares ante el tratamiento de los datos personales en el ámbito comercial. Por lo tanto, es la persona que tiene el conocimiento necesario tanto del ámbito tecnológico como del jurídico para garantizar el derecho a la protección de datos personales sin limitar la libre circulación de los mismos en pro del desarrollo económico.

A interpretación de lo que la Agencia Española de Protección de Datos ha definido, con respecto a los requisitos de conocimientos y habilidades del Delegado de Protección de Datos, se considera sujeto cualificado para la protección de los datos personales, a quien tenga un alto conocimiento de la Ley en materia de protección de datos personales –nacional e internacional–, ser una persona ética y profesional, así como tener conocimientos técnicos para la protección de los datos en relación a la implementación de mecanismos de seguridad y desarrollo por seguridad y por defecto.

Lo anterior va en relación a las “Directrices sobre los delegados de protección de datos (DPD)”[109], así como en relación a los artículos a los que dichas directrices hacen referencia en el *Reglamento General de Protección de Datos del Consejo de Europa*, documento donde se mencionan las funciones que debe desempeñar el delegado de protección de datos. Por ello, para desempeñar las funciones mencionadas, se entiende que requiere tener los conocimientos de las materias señaladas.

[109] *Cfr.* Agencia Española de Protección de Datos, Esquema de Certificación…, *Op. Cit.* p. 12-13.

No será necesario que cuente con carrera en el área de derecho o en el área de tecnologías, pues bastará con que se demuestre el conocimiento mediante una certificación en materia de protección de datos personales, que puede ser por algún ente certificador del país de que se trate, o por la Agencia Española de Protección de Datos como una de las más reconocidas y avanzadas en la materia, misma que ha establecido los criterios para la certificación de los delegados de protección de datos.

Una sola persona no podría llevar a cabo todas las funciones que la protección de datos personales requiere, lo que hace necesario que exista un área jurídica que pueda atender las controversias que se deriven del tratamiento de estos datos; el delegado de protección de datos deberá tener los conocimientos generales de las leyes para entender el contexto y poder implementar acciones de salvaguarda de los derechos, así como para el cumplimiento de la Ley; no obstante, deberá tener conocimientos en seguridad de la información y análisis de riesgos, así como conocimientos de informática forense para poder hacer ejercicios de trazabilidad de los datos, y con ello coadyuvar a las funciones del área jurídica para la solución de controversias.

Sujeto Organizado. Por su parte, el sujeto organizado serán todas las empresas comerciales que para el desarrollo de sus actividades económicas en el mercado requieren hacer recolección, tratamiento y almacenar datos personales, mismas que deberán contar con mecanismos que garanticen el derecho a la protección de datos personales, sea mediante su adhesión a códigos deontológicos o mediante la implementación de buenas prácticas, así como la adopción de mecanismos de seguridad administrativa, técnica y física.

Cabe precisar que, en la sociedad de la información, las tecnologías son un instrumento necesario para el desarrollo económico del país, pero que a menudo se convierte en un instrumento de violaciones a derechos humanos. Esto se debe contrarrestar con capacitación y difusión; capacitación al personal responsable de la protección de los datos personales y difusión de los derechos humanos en el sector social, pues sin el conocimiento de los derechos no se puede exigir su

respeto, y sin la capacitación para la protección de dicho derecho desde el ámbito técnico hasta el ámbito jurídico, no podrá garantizarse el respeto de dicho derecho.

*Lo maravilloso de aprender algo*
*es que nadie puede arrebatárnoslo*

*- B. B. King -*

# CAPÍTULO TERCERO

## RESULTADO DEL ANÁLISIS DE LOS AVISOS DE PRIVACIDAD

### *3.1. Sector de análisis y muestra de representación*

Antes de comenzar a analizar los avisos de privacidad de las empresas, es importante mencionar que las empresas que se eligieron para dicho análisis, fueron escogidas por el hecho de que, de alguna u otra manera realizan comercio en línea en cualquiera de sus modalidades que se mencionarán más adelante. De tal manera que siete de estas empresas se eligieron del listado de empresas finalistas concursantes al premio eCommerce Award[110], por lo que se espera que sus avisos de privacidad cuenten con elementos suficientes para cumplir con la normativa en materia de protección de datos personales.

Las empresas seleccionadas de este listado, desarrollan sus actividades en la industria turística, medios de comunicación y venta al menudeo. Los nombres de las empresas a las que se hace referencia en el párrafo anterior son: PriceTravel; Clickonero; Groupon; Interjet; Almundo; Elektra y Cinépolis, de las cuales se dará una pequeña reseña a continuación solo a manera de información genera de las mismas.

PriceTravel (www.pricetravel.com.mx), es una empresa que desarrolla sus actividades en el sector turístico, fue fundada en el año 2000 en ciudad de Cancún, Quintana Roo, México. "[…] Fue una de las primeras agencias de viajes a través del *Internet* que firmó acuerdos comerciales con algunas de las más importantes cadenas hoteleras, tales como Occidental Resorts, Camino Real y Riu"[111]. Actualmente ofrece servicios de trasportación venta de boletos aéreos y hospedaje y debido a su crecimiento ahora cuentan con oficinas en Acapulco y Puerto Vallarta.

---

[110] El Instituto Latinoamericano de Comercio Electrónico, eCommerce Institute, en conjunto con sus capítulos locales en América Latina instauró estos premios con el objetivo de reconocer a las empresas que cumplen con las buenas prácticas y con su constante trabajo hacen posible el desarrollo de la Economía Digital en México y la Región, https://ecommerceaward.org/estas-son-las-empresas-finalistas-ecommerce-award-mexico-2018/. Consultado: 22/12/2019.

[111] Price Travel, *Acerca de PriceTravel,* https://www.pricetravel.com.mx/info/acerca-nosotros. Consultado: 22/12/2019.

Clickonero, es una empresa de la cual no hay mucha información relacionada a la empresa, actualmente parece haberse fusionado con la empresa Outlet de Viajes (www.outletdeviajes.mx), empresa que desarrolla sus actividades comerciales en el sector turístico, realiza venta en línea de boletos de avión y tours turísticos. Sin embargo, al momento de identificar quien será el responsable del tratamiento de los datos personales, no se especifica claramente, lo que hace pensar que su aviso de privacidad está violando el derecho a la libre autodeterminación informativa de los usuarios, lo cual genera especial interés e inquietud por esta empresa.

Groupon (www.groupon.com.mx), en su capítulo de Groupon México, es una empresa constituida con el bajo la razón social de Needish México, S. de R.L. de C.V., misma que en el año 2018[112] se fusionó con la empresa Peixe Urbano –empresa brasileña– dando como resultado Peixe México con la ya mencionada razón social. Su actividad es diversa, ya que vende boletos de viajes, productos diversos, además otras empresas pueden contratar publicidad en este sitio de e-commerce.

Interjet (www.interjet.com.mx), esta es una empresa mexicana, constituida en el año 2005 bajo la denominación de ABC Aerolíneas, S.A de C.V., el producto que ofrece son vuelos comerciales a destinos tanto nacionales como internacionales, gracias a las alianzas que han creado con otras "[…] aerolíneas como, Alitalia, All Nippon Airways (ANA), American Airlines, British Airways, Iberia, Grupo LATAM Airlines, Lufthansa, Hainan Airlines, Japan Airlines y EVA Air para presentarte un mundo de posibilidades al momento de planificar un viaje"[113].

Almundo (almundo.com.mx) es una agencia de viajes que cuenta con tres sucursales en la Ciudad de México, la cual se constituyó bajo la denominación de TKT Mas Operadora, S.A. de C.V., en su sitio web anuncia la venta en línea de vuelos, alojamiento, paquetes, actividades, seguros, renta de coches, cruceros y circuitos.

---

[112] *Cfr.* Peixe, *Acerca de Peixe,* https://www.groupon.com.mx/e/acerca-de, Consultado: 22/12/2019.
[113] Interjet, *Quienes somos,* https://www.interjet.com/es-mx/experiencia-interjet/viajando-con-interjet/quienes-somos. Consultado: 22/12/2019.

Por su parte, Elektra (www.elektra.com.mx) es una empresa de la división del negocio comercial de Grupo Elektra[114], dedicada a la venta al menudeo de una variada gama de productos de electrónica, línea blanca, electrodomésticos, muebles, telefonía celular, motocicletas, cómputo y transferencias de dinero. Al ser una empresa que pertenece a un grupo de empresas, da la impresión de que los datos recolectados en relación a los clientes, podrían ser compartidos sin mayor problema entre las empresas del mismo grupo ya que la misma Ley en materia de protección de datos personales así lo establece en el artículo 37[115], por ello, el interés de esta empresa se centra en observar el cumplimiento respecto a la libre autodeterminación informativa.

La última empresa de este listado es Cinépolis (cinepolis.com), empresa mexicana constituida bajo la razón social de Cinépolis de México, S.A. de C.V., considerada una de las empresas más importantes de México en la industria de la cinematografía, que si bien, no es una productora de películas, si es la empresa líder en exhibición de contenido cinematográfico. En su portal web, además de vender boletos en línea, también se promocionan otros servicios de grupo Cinépolis como, Sala de Arte[116], Cine Park[117], CinépolisVR[118] y Cine Cash[119], los cuales se enuncian por ser servicios que resaltan entre la variada gama de servicios

---

[114] *Cfr.* Grupo Elektra, *Acerca de Grupo Elektra,* http://www.grupoelektra.com.mx/es/sustentabilidad/quienes-somos.html. Consultado: 22/12/2019.

[115] *Cfr.* Ley Federal de Protección de Datos…, *Op. Cit.* Artículo 37.

[116] Se retoma el texto de la página oficial de Cinépolis, donde se define que la "Sala de Arte Cinépolis® es un espacio permanente en 25 salas de la República Mexicana en donde podrás descubrir propuestas cinematográficas de los autores más reconocidos del cine mundial, las películas celebradas en festivales alrededor del mundo, así como documentales y películas clásicas del cine".

[117] Se retoma el concepto de la página oficial de internet, donde se menciona que "Cinema Park es el primer concepto de Entretenimiento Educativo - Edutainment en salas de Cine en América que, en colaboración con Fundación Cinépolis, busca generar cambios positivos en las personas creando inmersión en experiencias multisensoriales, interactivas y educativas en el cine a través de sus tours temáticos".

[118] *Cfr.* Cinepremiere, *Cinépolis VR ofrecerá experiencias de videojuegos de realidad virtual,* 2017, https://www.cinepremiere.com.mx/cinepolis-vr-experiencias-realidad-virtual.html. Consultado: 21/12/2019

[119] CineCash "es tu nueva forma de pago en línea que te permite acceder a preventas exclusivas, rentar tus películas en Cinépolise Klic, elegir tu lugar en la sala comprando tus boletos, sin necesidad de una tarjeta de crédito 0 débito, y mucho más desde tu PC, Facebook 0 cualquier App de Cinépolise", https://cinepolis.com/HTML/Otros/landing-cinecash/cinecash.html. Consultado: 20/08/2019.

relacionados a la exhibición de películas, que es la actividad principal por la que se ha dado a conocer esta empresa por varios años.

De igual manera se seleccionaron tres empresas más, el criterio de elección de dichas empresas se basó en analizar sus portales web para verificar que contaran con un sistema de e-commerce o algún formulario mediante el cual hagan recolección de datos personales, que fueran empresas en la categoría de microempresas y que sus ventas fueran al menudeo, asimismo, se tuvo el cuidado de verificar que dichas empresas operaran en la ciudad de Morelia, Michoacán. A continuación, se enuncian las empresas seleccionadas y se hará una breve reseña de las mismas.

Duran Autopartes (www.duranautopartes.com), es una empresa de venta al menudeo de accesorios y refacciones para coche, en su portal de web se observa un formulario de registro, un carrito de compras, así como el menú de navegación organizado por los tipos de productos que oferta. Se trató de localizar un aviso de privacidad, pero no se pudo identificar, lo que hace pensar que no cuenta con dicho requerimiento de la Ley.

Proser Soluciones (proser.mx), es una empresa constituida bajo la denominación de Perisol S.A. de C.V., desarrolla su actividad en el sector del comercio de productos y servicios de tecnologías de la información; dicha empresa pertenece a la clasificación de las microempresas, es de origen michoacano y sus oficinas se encuentran en la ciudad de Morelia. En su portal web tiene implementada una plataforma de e-commerce, en la que se pueden añadir productos al carrito de compras, realizar pagos en línea con tarjeta de crédito o débito e introducir los datos de envío para poder recibir los productos en la comodidad del domicilio del cliente.

Al igual que el caso anterior, se exploró el sitio web en busca del aviso de privacidad sin lograr encontrar dicho documento, hecho por el que se presupone que está incumpliendo la Ley, toda vez que hace recolección de datos personales, entre los cuales se incluyen datos que requieren del consentimiento del cliente para ser tratados, y no cuenta con un aviso de privacidad donde informe a los usuarios sobre el tratamiento de los datos recolectados.

Por último, es turno de la empresa Sublimarte, la cual tiene dos portales en *Internet,* que si bien en ninguno de ellos cuenta con un e-commerce, si cuenta con un formulario de contacto, resulta de interés notar que aunque en estos portales si existe un apartado de “política de privacidad” y “política de cookies”, no está personalizado acorde a la empresa, de tal manera que, al igual que las dos empresas anteriores están incumpliendo con la obligación de informar al usuario mediante el aviso de privacidad, sobre el tratamiento de los datos personales.

Así entonces, se ha establecido que el total de empresas a analizar es de diez, de las cuales no solo se realiza un análisis de los avisos de privacidad, sino, también de los portales web, con la finalidad de detectar todos los formularios mediante los cuales solicitan la introducción de datos a los usuarios y el motivo de la recolección, para posteriormente, verificar si mediante sus avisos de privacidad informan adecuadamente sobre los datos recolectados y su tratamiento.

Es preciso recordar que, al momento de hacer compras en línea, el método de pago por excelencia es la tarjeta de crédito o débito. Sin embargo, los sistemas de pagos por lo regular son gestionados por empresas especializadas, ello se debe a la seguridad que éstas han implementado para la realización de transacciones de manera segura, pues una de las principales preocupaciones de las empresas, es garantizar que las transacciones de dinero se hagan de manera segura, ya que en caso de sufrir una vulneración en la que se extraiga información del cliente o su dinero, el responsable debe reembolsar el dinero al cliente.

Así entonces, todas las compras que se realizan en línea tienen dos puntos de tratamiento de datos personales, uno por la empresa que realiza la venta y otro por la empresa que gestiona la transacción de dinero. En este caso la empresa que realiza la transacción de dinero debe realizar el tratamiento de los datos personales para autenticar la transacción y dar trazabilidad a la información, pero en este caso quien está obligado a informar de dicho tratamiento es el responsable, pues no olvidemos que la empresa que efectúa la transacción estará ejecutando una orden del responsable, por cuyo servicio cobrará una comisión al responsable, dejando a dicha empresa el papel de encargado, de acuerdo a lo establecido en la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares.*

Lo anterior es importante puesto que, aunque las empresas que realizan las transacciones, como PayPal, Google Wallet, Amazon Payments, Dwolla o Authotize.Net, cuentan con sus propios avisos de privacidad, esto no le quita la responsabilidad a la empresa que está realizando la venta del producto o servicio, de informarle al cliente sobre dicho tratamiento, pues en la mayoría de los casos, al usar estas aplicaciones de pagos, la información puede salir del territorio nacional, sea porque los servidores de dichas aplicaciones residen en otro país o porque tienen espejos –servidores de respaldo– en otros países, por ello es importante informar de manera adecuada sobre dicho tratamiento o compartición de información, así como requerir el consentimiento acorde a los datos que serán transferidos.

Amén de las plataformas de pago, las empresas que realizan comercio electrónico no solo tratan información de ciudadanos del territorio nacional, –en este caso hablamos de México– sino, también cabe la posibilidad de que, gracias a las bondades de la tecnología de comercio en línea, ciudadanos de otros países puedan comprar productos a las empresas mexicanas sin que éstas comercialicen sus productos directamente en dichos países, lo que dará como resultado el flujo transfronterizo de datos personales e incluso la transferencia[120] de datos a un tercero en el país de destino donde se alojarán los mismos, pues como ya se analizó en el primer capítulo, los prestadores de servicios de cómputo en la nube actúan como un tercero en el tratamiento de los datos personales, y sus términos de uso de los servicios son aceptados mediante contratos de adhesión que en su mayoría, favorecen a dichas empresas tecnológicas.

En relación al caso anterior, lo que la empresa deberá dejar en claro es lo referente a las cuestiones fiscales, es decir, si esta no cuenta con una filial en el país de origen del cliente, no estará en condiciones de facturar el producto al cliente. De la misma manera los costos de envió deberán especificarse al momento de hacer la compra, ya que si no es un país donde se comercializa habitualmente, será

[120] La Ley Federal de Protección de Datos Personales en Posesión de los Particulares define la transferencia como "Toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento", *Op. Cit.* Art. 3, Frac. XIX.

una limitante el método de envío, pues si no cuenta con dicho servicio al país de destino, no debe permitir que el cliente pueda concluir la compra en línea.

Por otro lado, si existen las condiciones para poder concretar las transacciones comerciales, se debe tener el cuidado de informar claramente en el aviso de privacidad, sobre el destino de los datos y las condiciones de su tratamiento, pues en el supuesto que se plantea, podrían darse las condiciones para la transferencia a un tercero que gestione la transacción del dinero, así como para el tratamiento de datos de una persona de origen extranjero, lo cual supone un tratamiento con apego a la legislación del país de origen del titular de los datos tratados.

Otro supuesto es que las empresas mexicanas, mediante sus portales web realicen comercio electrónico en otros países de manera habitual, en cuyo caso podrán también hacer campañas publicitarias en esos lugares, por ejemplo, en Europa, bajo el supuesto de que la empresa tenga una filiar en dicho país, estaría en condiciones de poder facturar a los ciudadanos por la compra de sus productos, lo que da como resultado también la necesidad de compartir los datos entre las empresas filiales, es decir la empresa situada en Europa, pueden remitir[121] y/o compartir los datos con la empresa en México, para cuestiones contables y administrativas, sin que ello requiera del consentimiento del titular.

No obstante, esto debe especificarse en el aviso de privacidad, –el cual deberá está adaptado al idioma local donde se realice dicha actividad comercial– en un apartado dedicado denominado, “con quien compartimos tus datos personales”, en donde se especifique claramente con que empresas se comparten los datos personales y para qué fines. Cabe señalar que, en este supuesto, la empresa que asume la responsabilidad es la empresa del país donde se recaban los datos y asume la responsabilidad por la transferencia –cuando se use el servicio de un tercero– y la remisión de los datos a la empresa mexicana cuando estos sean compartidos o enviados a la empresa situada en México.

En relación al supuesto anterior y al margen de este trabajo, se debe observar el *Reglamento General de Protección de Datos del Consejo de Europa*, así como leyes

[121] El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares define la remisión como "La comunicación de datos personales entre el responsable y el encargado, dentro o fuera del territorio mexicano", *Op. Cit.* Art. 2, inciso d, Frac. IX.

reglamentarias, convenios –Convenio 108– así como los acuerdos sobre protección de datos personales, de tal manera que, el libre flujo de información –flujo transfronterizo– no supone una violación a los derechos humanos cuando se hace acorde a lo establecido por la Ley, pues no olvidemos que la circulación de la información es una condición necesaria para el desarrollo económico.

En el mismo tenor, la OCDE ha establecido desde 1980 las Directrices que regulan la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales, haciendo hincapié en que se debe "[…] evitar que aparezcan, en nombre de la protección de la privacidad, obstáculos injustificados para los flujos transfronterizos de datos personales"[122], ello con la intención de propiciar el comercio entre las naciones con las únicas limitantes del tratamiento de los datos personales, que garanticen la seguridad y el respeto de los derechos de los consumidores.

### *3.1.1. Relación entre comercio electrónico y tratamiento de datos*

Es posible que en ocasiones escuchemos hablar de negocios en línea y de comercio electrónico como sinónimos. Sin embargo, es importante señalar que para este estudio se entenderá al comercio electrónico como todo intercambio de valores[123] mediante plataformas digitales, esto es, las operaciones de compraventa de productos y servicios en el modelo de comercio de negocio a consumidor B2C (business to consumer, por sus siglas en inglés) que se explicará más adelante; al hacer referencia al intercambio de valores, nos referimos a transacciones comerciales en las que se sobreentiende que debe existir un pago del cliente a la empresa, a cambio de un producto o servicio a través de plataformas web especializadas para tales efectos.

Así entonces, la relación entre comercio electrónico y el tratamiento de datos personales en la nube, podría tener una relación mucho más estrecha de lo que se piensa, pues al momento de hacer uso de cualquier plataforma de e-commerce,

---

[122] OCDE, *Directrices de la OCDE que regulan la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales,* Ministerio de Administraciones Públicas, 1980, p. 3, http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf. Consultado 24/12/2019.
[123] *Cfr.* Kenneth C., Laudon y Guercio Traver…, *Op. Cit.* p. 13.

estamos utilizando alguna nube, es decir, un servidor que procesará los datos personales para poder completar la operación de compraventa, esto, además supone la compartición de los datos con la empresa gestora de las transacciones comerciales, en caso de usar el servicio de un tercero para tal efecto. En caso de que dicha transacción la gestione directamente el responsable, tendría que tomarse en cuenta qué tipo de servicio web se utiliza para el alojamiento de los datos, es decir, si es prestado por un tercero o es propietario.

Ahora bien, sea quien sea el propietario del sistema que se utilice para la gestión de los pedidos y las transacciones de dinero, lo que se debe tener presente en el comercio electrónico, es el tipo de plataforma que se utiliza para las operaciones comerciales, pues se entiende que el comercio electrónico funciona mediante plataformas web conectadas a la red de *Internet,* característica que hace de estas plataformas un sistema ubicuo al no tener la certeza de dónde se almacenarán los datos, la ruta que se sigue para llegar al destino final y si existen copias dentro o fuera del territorio nacional.

Otro elemento importante a tener en cuenta, son los proveedores del servicio de *Internet,* pues en México, quienes prestan estos servicios son las empresas de telecomunicaciones, las cuales pueden operar concesiones de prestación de servicio de radiodifusión[124] o de telecomunicaciones[125], lo cual resulta importante al momento de analizar el tratamiento de los datos personales puesto que, a las empresas de telecomunicaciones se les ha requerido, mediante la *Ley Federal de Telecomunicaciones y Radiodifusión*, que almacenen los datos de identificación de

[124] La Ley Federal de Telecomunicaciones y Radiodifusión define la Radiodifusión como "Propagación de ondas electromagnéticas de señales de audio o de audio y video asociado, haciendo uso, aprovechamiento o explotación de las bandas de frecuencia del espectro radioeléctrico, incluidas las asociadas a recursos orbitales, atribuidas por el Instituto a tal servicio, con el que la población puede recibir de manera directa y gratuita las señales de su emisor utilizando los dispositivos idóneos para ello", *Ley Federal de Telecomunicaciones y Radiodifusión,* DOF, reformada 15-06-2018, Art. 3, p. 6, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_020419.pdf. Consultado: 11/01/2019.

[125] La Ley Federal de Telecomunicaciones y Radiodifusión define las Telecomunicaciones como "Toda emisión, transmisión o recepción de signos, señales, datos, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radioelectricidad, medios ópticos, físicos u otros sistemas electromagnéticos, sin incluir la radiodifusión", *Ley Federal de Telecomunicaciones…, Ibidem, Art. 3, p. 8.*

los suscriptores por un lapso de 24 meses[126], periodo en el que las autoridades competentes podrán acceder o solicitar a dicha empresa una copia de la información concerniente a una personas, como medio probatorio ante cualquier controversia.

Esto supone que, ante las operaciones de comercio electrónico, además de transferir los datos a un tercero, dentro o fuera del territorio nacional, remitirlos o compartirlos con alguna filial, estos datos también se estarán transfiriendo al prestador de servicios de *Internet* de manera innegable y como condición del uso de la red de telecomunicaciones, por tanto, sin importar si las tecnologías utilizadas en el proceso de compraventa de productos y servicios en línea son propietarias de la empresa, cierta parte de los datos personales que identifican al titular, serán transferidos al proveedor del servicio para su conservación en los términos establecidos por la Ley.

Si bien, este tratamiento encaja con lo dispuesto en el artículo 37, fracción I, de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* donde refiere que la transferencia de los datos podrá llevarse a cabo "Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte"[127], no deja de lado la obligación de informar dicho tratamiento, pues los usuarios de los servicios en línea no están obligados a saber sobre el proceso, mientras que el responsable sí está obligado a informárselo mediante el aviso de privacidad.

No obstante, pese a que este tratamiento está previsto por la Ley, cabe la duda de si la información que se recolecta y almacena cumple con el principio de proporcionalidad, pues se ha sabido que las empresas de telecomunicaciones recolectan más información de la necesaria para la prestación del servicio[128], en cuyo caso, estaríamos hablando de una intromisión arbitraria a la vida privada de los usuarios de sus servicios por un particular, es decir, por la empresa prestadora del servicio de telecomunicaciones.

---

[126] *Cfr.* Ibidem, Art. 190, p. 78.
[127] *Ley Federal de Protección de Datos Personales…, Op. Cit.* Art. 37, p. 9.
[128] *Cfr.* Pérez Gil, Julio, "El Nuevo Papel De La Telefonía Móvil En El Proceso Penal: Ubicación y Perfiles De Desplazamiento." *El Proceso Penal En La Sociedad De La Información. Las Nuevas Tecnologías Para Investigar y Probar El Delito,* Universidad de Burgos, 2012. pp. 110–111, https://www.academia.edu/33767738/El_nuevo_papel_de_la_telefon%C3%ADa_m%C3%B3vil_en_el_proceso_penal_ubicaci%C3%B3n_y_perfiles_de_desplazamiento?source=swp_share, Consultado: 11/01/2020

Aunado a lo anterior, se suma la recolección masiva de los datos personales por las empresas tecnológicas propietarias de los algoritmos de búsqueda, sector liderado por Google, pues al usar los servicios, en los motores de búsqueda dejamos grandes cantidades de datos personales que nos pueden identificar como usuarios únicos en la red[129], permitiendo a dichas empresas generar perfiles digitales para ofrecer a sus anunciantes mejores servicios de publicidad focalizada, aumentando las posibilidades de éxito para las empresas contratantes de sus servicios.

Lo anterior dificulta el ejercicio del derecho a la protección de datos personales por el desconocimiento de los usuarios, quienes al no saber cómo es que operan realmente estas tecnologías de comercio electrónico, ignoran que sus datos podrían estar viajando por el mundo, que son tratados por otras empresas como resultado del uso de un servicio, que pueden permanecer fuera del territorio nacional y que en ocasiones esto ocurre sin su consentimiento.

Incluso, los mismos responsables del tratamiento de los datos desconocen muchas de estas cuestiones, sobre todo si hablamos de las microempresas, que como ya se ha señalado en el primer capítulo, son la mayoría de las empresas que sostienen la economía de México, y que como hemos dado cuenta en párrafos anteriores, muchas de ellas no cuentan con los avisos de privacidad, lo que supone una violación al derecho a la autodeterminación informativa.

Por ello, se considera importante hacer una diferenciación respecto a los tipos de comercio electrónico, esto con la intención de puntualizar los tipos de consentimiento que se requieren de los clientes al momento de hacer recolección de datos personales, pues el tipo de consentimiento –tácito, expreso o expreso y por escrito– depende de los datos que se recolectan. Por su parte, los datos que se recogen, dependen de la modalidad de comercio electrónico que la empresa realiza.

*A. Tipos de comercio electrónico*

En el comercio electrónico existen distintas clasificaciones según el tipo de clientes y oferentes de los productos y servicios. Resulta importante señalarlo, toda

[129] *Cfr.* Peirano, Martha, El enemigo…, *Op. Cit.* pp. 93–96.

vez que las empresas que nos interesa analizar son aquellas que venden sus productos y servicios a los consumidores finales y no a otras empresas, en cuyo caso se trataría de personas morales que no gozan del derecho a la protección de datos personales.

Dicho la anterior, nos referiremos al modelo de comercio electrónico de negocio a consumidor B2C[130] (business to consumer, por sus siglas en inglés), el cual centra sus esfuerzos por realizar las ventas directamente al consumidor, mediante el uso de plataformas digitales que permitan promocionar sus productos y servicios en la web, y mediante sistemas de comercio electrónico realizar las operaciones comerciales en el ciberespacio, modelo en el que encajan las empresas seleccionadas para el análisis de los avisos de privacidad.

El siguiente modelo de negocio es el denominado como comercio electrónico de negocio a negocio B2B[131] (business to business, por sus siglas en inglés), este modelo de comercio electrónico busca vender sus productos y servicios a otros negocios minoristas, lo que supone que el tratamiento de datos sería de las personas morales, que si bien, los datos de las personas de contacto podrían requerir de la protección de los datos personales conforme a la Ley, no sucede lo mismo con los datos de las empresas, por tanto, este tipo de empresas quedarán excluidas para este estudio puesto que, lo que interesa es analizar el cumplimiento de la Ley en cuanto al derecho a la protección de datos personales.

En cuanto al modelo de negocio de comercio electrónico de consumidor a consumidor C2C[132] (consumer to consumer, por sus siglas en inglés), es un modelo en el que los consumidores venden a los consumidores, un ejemplo podría ser Mercado Libre o los portales de anuncios de clasificados, la característica que se debería de cumplir en este caso es que las plataformas permitan realizar las transacciones comerciales, desde la puesta a disposición de los productos en línea hasta el cobro y entrega de los mismos en el domicilio de los consumidores finales.

Respecto a los modelos de comercio electrónico social y comercio electrónico móvil, no ahondaremos mucho, pues basta señalar que el primero de ellos se refiere

---

[130] *Cfr. KENNETH C., Laudon y GUERCIO TRAVER, Carol, E-commerce 2013…, Op. Cit. p. 22.*
[131] *Cfr. Idem.*
[132] *Cfr. Idem.*

al comercio electrónico en redes sociales y relaciones sociales, mientras que el segundo es el comercio electrónico en cualquiera de sus modalidades, pero desde los dispositivos móviles, como tabletas, computadoras portátiles, teléfonos inteligentes, lo cual requiere características especiales para poder operar de manera amigable y correcta en distintos sistemas operativos y en distintas resoluciones de pantalla[133].

Por último, el comercio electrónico local[134] es una modalidad de comercio electrónico donde los esfuerzos se enfocan en atraer a los consumidores a los establecimientos físicos, en este caso resulta de interés debido a que, en ocasiones, las empresas que realizan este tipo de comercio electrónico implementan formularios de contacto en sus portales web, mediante los cuales los consumidores pueden interactuar de manera asíncrona con los trabajadores de dichas empresas. Incluso mediante este tipo de comercio electrónico podrían realizarse los pedidos y concretar las transacciones en el sitio geográfico donde se localiza el negocio, en cuyo caso, se presupone un tratamiento de datos personales en algún tipo de nube.

Dicho lo anterior, parece pertinente indicar que los negocios de los cuales se analizarán los avisos de privacidad, encajan en los modelos de comercio electrónico B2C y comercio electrónico local. También resulta importante señalar que la relación entre estos modelos de comercio con el tratamiento de datos personales en la nube, deriva de las plataformas utilizadas y “el modelo de computación cliente/servidor”[135].

*B. Características del comercio electrónico*

A consecuencia del uso de las tecnologías de la información y comunicación para el comercio electrónico, derivan ocho características del comercio electrónico, que dan la pauta para entender la relación entre comercio electrónico y tratamiento de datos personales en la nube. Dichas características se sintetizan a continuación.

---

[133] *Cfr. Ibidem.* pp. 22–23.
[134] *Cfr. Idem.*
[135] *Cfr. Ibidem.* p. 128, figura 3.7.

a. Ubicuidad

La ubicuidad[136] es una característica en común con la tecnología de cómputo en la nube, esto se debe a que los modelos de comercio electrónico no se limitan a un establecimiento físico, sino que, su presencia en el ciberespacio abre las fronteras para llegar a los consumidores a través de dispositivos móviles o computadoras de escritorio. Cabe señalar que los datos que las empresas requieren para poder concretar las transacciones comerciales, se alojan en un servidor, del cual se desconoce la ubicación geográfica específica, esto es lo que le da la característica de ubicuidad al comercio electrónico.

b. Alcance global

El comercio electrónico tiene un alcance global, no se limita a una zona geográfica, así, personas de cualquier país y cultura podrían tener la posibilidad de adquirir productos y servicios de su interés, sin importar donde se localiza la empresa que los oferta. "[…] El mercado virtual incluye a miles de millones de clientes y millones de negocios potenciales en todo el mundo"[137], esto gracias a las bondades de las tecnologías web e *Internet*.

c. Estándares universales

A diferencia de los estándares de comercio tradicional, en el comercio electrónico los "estándares tecnológicos"[138] son universales, es decir, en cualquier parte del mundo que se realiza comercio electrónico se utilizan las mismas tecnologías de *Internet* y de la web para realizar las transacciones, lo que hace común en cualquier modelo de comercio electrónico el tratamiento de los datos personales. De tal manera que, si los estándares son internacionales, la legislación que regula dicho tratamiento debería de tener similitudes, pues regulan el tratamiento en el mismo entorno tecnológico.

---

[136] *Cfr. Ibidem,* p. 13.
[137] *Ibidem,* p. 15.
[138] *Idem.*

d. Riqueza e interactividad

Estas son dos características distintas, de las cuales, la primera hace referencia a la riqueza del contenido que se puede transmitir mediante video, audio y texto que se integran al *marketing* digital. Por su parte, la interactividad hace referencia a la interacción que hace coparticipes a los consumidores "[…] en el proceso de distribución de bienes en el mercado"[139]. Para ello se requiere también del tratamiento de los datos personales, útil para encaminar las acciones mercadotécnicas y la innovación, o creación de nuevos productos acorde a las necesidades de los consumidores.

e. Densidad de la información

"Internet y la web incrementan en gran medida la densidad de la información"[140], esto es mediante estas tecnologías es posible la circulación de grandes cantidades de datos, lo que permite a las empresas poner al alcance de los consumidores la información suficiente de sus productos y servicios, pero a la vez, los consumidores entregan grandes cantidades de información a las empresas de manera gratuita, y gracias al tratamiento de dichos datos mediante tecnologías, las empresas pueden obtener un beneficio económico y generan mayor competencia en el mercado.

f. Personalización y adecuación

Como ya se ha mencionado anteriormente, el tratamiento de los datos personales tales como los patrones de navegación del usuario en *Internet,* las compras anteriores, el género o las conductas en las redes sociales, permite a las empresas ajustar "[…] el mensaje al nombre de una persona, a sus intereses y compras anteriores. [Lo que permite a las empresas personalizar el] anuncio publicitario basado en el perfil [digital] del consumidor"[141].

---

[139] *Idem.*
[140] *Ibidem.* p. 17.
[141] *Ibidem.* p. 18.

g. Tecnología social

"Las nuevas tecnologías de *Internet* y del comercio electrónico"[142]. permiten que los consumidores, mediante redes sociales, creen su propio contenido, pues a menudo vemos cómo los consumidores en redes sociales muestran videos usando algún producto, exponiendo sus experiencias del uso de los mismos o compartiendo información de los productos de su interés.

Esta es una característica del comercio electrónico, pues como ya se mencionaba, el comercio electrónico social no solo permite a las empresas hacer marketing en redes sociales, sino que los mismos consumidores son parte activa del *marketing* de las empresas, esto genera un rastro digital de los consumidores que puede ser aprovechado para posteriores campañas publicitarias.

Todo lo anterior es importante puesto que el comercio electrónico, por sus características, para poder operar de manera eficiente como lo ha venido haciendo hasta ahora, requiere del tratamiento y análisis de los datos personales, mismos que pueden ser recopilados mediante los sistemas de transacciones en línea y/o formularios web, propios de la plataforma de comercio electrónico, así por tecnologías secundarias incrustadas en las plataformas digitales, tales como *Big Data, cookies, beacons* u otros mecanismos de minería de datos; actividad que a menudo los consumidores pasan por desapercibida, pero que repercute directamente en la información publicitaria que recibe día a día en los dispositivos electrónicos, constituyendo en buena medida una violación a la privacidad, derivado de la intromisión a su vida privada mediante las tecnologías de la información.

Si bien en cuanto a la protección del consumidor ya existen elementos que brindan protección en el comercio electrónico, algunos de estos elementos quedan en recomendaciones, –que habríamos de revisar su cumplimiento– buenas prácticas o códigos autorregulatorios por las empresas comerciantes de productos y servicios, acciones que en gran parte están orientadas a generar confianza de los consumidores, y así fomentar el crecimiento del comercio electrónico en aras de fortalecer la economía, lo cual, en tal sentido, no es criticable.

---

[142] *Ibidem.* pp. 18–19.

Ejemplo de ello, es la *Recomendación del Consejo de la OCDE relativa a los Lineamientos para la Protección al Consumidor en el Contexto del Comercio Electrónico* de 1999*,* en donde se consideran normativas relativas a la protección del consumidor y a la privacidad. En relación a la autodeterminación informativa, parecen relevantes los textos extraídos de los Principios Generales, apartado II, relacionados a la libertad del consumidor para aceptar o rechazar la publicidad de la empresa, en tales párrafos se lee:

> Las empresas deben tener la capacidad de comprobar cualquier afirmación expresa o implícita, durante todo el tiempo en que ésta sea hecha, y mantener esta capacidad durante un tiempo razonable, una vez concluida dicha declaración.
>
> Las empresas deben desarrollar e implementar procedimientos efectivos y fáciles de usar, que permitan a los consumidores manifestar su decisión de recibir o rehusar mensajes comerciales no solicitados por medio del correo electrónico[143].

Esto tiene relación con uno de los elementos que se deben incluir en el aviso de privacidad y la autodeterminación del titular para decidir si acepta o no dicho envío de publicidad, en cuyo caso, dicha condición no puede formar parte de la finalidad primaria del tratamiento de los datos personales, cosa que parece no ser tomada en cuenta, pues en la mayoría de los avisos de privacidad se especifica que la información podrá ser usada con finalidades secundarias que por lo regular corresponden a usos mercadotécnicos y publicitarios.

En relación a la protección de los datos personales, el apartado VII denominado “Privacidad”, pese a que no desarrolla ampliamente las recomendaciones, refiere que tanto las empresas como los consumidores deben conducirse conforme a los *Lineamientos que Regulan la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales de la OCDE* de 1980[144], y deben tomar en cuenta la *Declaración Ministerial de la OCDE sobre Protección de la Privacidad en Redes Globales* de 1998, en el que declaran entre otras cosas que, “tomarán medidas necesarias, dentro de sus respectivas reglamentaciones y prácticas, para garantizar

---

[143] OCDE, *Recomendación del Consejo de la OCDE relativo a los Lineamientos para la Protección al Consumidor en el Contexto del Comercio Electrónico,* OCDE, 1999, p. 6, https://www.oecd.org/sti/consumer/34023784.pdf. Consultado: 07/01/2020.

[144] OCDE, *Directrices de la OCDE que regulan la Protección de la Privacidad…, Op. Cit.* pp. 5–6.

que las Directrices sobre la Intimidad de la OCDE sean llevadas a efecto de forma eficaz en relación con las redes globales"[145].

En virtud de que México es parte de la OCDE, está obligado a observar todas las recomendaciones y directrices que dicho organismo elabore, por tanto, dichas directrices, la declaratoria, así como las recomendaciones en materia de criptografía, deberán ser tomadas en cuenta para adecuar la legislación en materia de protección de datos personales ante el comercio electrónico, que supone el flujo de información y el tratamiento por los responsables –empresas–. Es preciso recordar que, cuando se habla de comercio electrónico, se supone un inherente flujo transfronterizo de datos personales para concretar las transacciones comerciales.

En el ámbito legislativo podemos encontrar elementos jurídicos de protección al consumidor, a nivel local –hablando de México–, en la *Ley Federal de Protección al Consumidor*[146]*,* en el *Código de Comercio*[147]*,* en la *Ley de Protección y Defensa al Usuario de Servicios Financieros*, así como por el *Código Penal Federal*.

Sumado a lo anterior, se cuenta con la Procuraduría Federal del Consumidor (PROFECO), que incluso ha implementado el Programa de Monitoreo de Tiendas Virtuales[148] para orientar a los consumidores sobre la confiabilidad de las tiendas en línea; la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF), que cuentan con un micro sitio[149] con recomendaciones para los consumidores.

Sin embargo, pese a las recomendaciones y a la normativa en cuanto a la protección del consumidor, específicamente en lo que respecta a la protección de sus datos personales que son tratados por las empresas que realizan comercio electrónico, mismos que son almacenados en plataformas de cómputo en la nube, y en relación a la garantía de respeto al derecho humano a la protección de los

---

[145] OCDE, *Declaración Ministerial relativa a la Protección de la Intimidad en las redes Globales, OCDE,* 1998, p. 4, http://www.oas.org/es/sla/ddi/docs/Declaracion_OCDE_Proteccion_Intimidad_redes.pdf. Consultado: 07/01/2020.

[146] Ley Federal de Protección al Consumidor, reformada, DOF, 12-04-2019.

[147] Código de Comercio, reformado, DOF, 28-03-2018.

[148] PROFECO, *Monitoreo de Tiendas Virtuales,* 2019, [en línea], https://www.gob.mx/profeco/documentos/monitoreo-de-tiendas-virtuales-114564?state=published. Consultado: 05/01/2020.

[149] *Cfr.* CONDUSEF, *Comercio Electrónico,* [en línea], https://www.condusef.gob.mx/gbmx/?p=comercio-electronico. Consultado: 20/03/2020.

datos personales, queda la duda de si las empresas están haciendo un uso malicioso, doloso, abusivo o, si por el contrario, existe desconocimiento de la Ley, por lo que es importante analizar si se está garantizando el derecho a la libre autodeterminación informativa al titular de los datos, o si se está sometiendo a condiciones violatorias de sus derechos ante el uso de plataformas de comercio electrónico.

### *3.1.2. Parámetros de análisis en los avisos de privacidad*

Como ya se ha dicho anteriormente, el aviso de privacidad es el documento físico, electrónico o en cualquier otro formato existente, o que pueda existir en el futuro, mediante el cual el responsable debe informar al titular sobre la existencia del tratamiento de datos personales, las características específicas de dicho tratamiento, es decir, las finalidades, si se comparten, transfieren o tratan mediante tecnologías automatizadas, así como los procedimientos para ejercer los derechos ARCO.

Consecuentemente, el análisis de los avisos de privacidad se centra en la búsqueda del cumplimiento a tal deber informativo, ello con la intención de constatar el cumplimiento de lo dispuesto por la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, así como en el análisis de los portales web, para detectar posibles tratamientos de datos personales que deban ser informados mediante el aviso de privacidad.

A partir del planteamiento anterior, será posible generar un indicador de cumplimiento por parte de las empresas analizadas, respecto al cumplimiento de los principios y deberes, que, a su vez, dará la pauta para cuestionar sobre la idoneidad de los avisos de privacidad en relación a la normativa mexicana y europea.

#### *A. Apego a los principios de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*

A continuación se presenta el análisis de los avisos de privacidad, el cual determina el cumplimiento de lo que se establece en cada uno de los ocho principios

que rigen el tratamiento de datos personales, según la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* dicho resultado se presenta en la tabla 3.1, la cual contiene los nombres de las empresas en la primera columna y los principios en las columnas sucesivas, marcando con una ✓ debajo de cada principio en el que se considera que le empresa cumple con lo establecido en la Ley; una ✗ en el caso de que no cumpla y un ? en caso de no ser posible, –mediante el aviso de privacidad–, determinar el cumplimiento de dicho principio.

| Empresa | Licitud | Lealtad | Consentimiento | Calidad | Finalidad | Proporcionalidad | Responsabilidad | Información |
|---|---|---|---|---|---|---|---|---|
| **PriceTravel** | ✓ | ? | ✓ | ? | ✓ | ✗ | ✓ | ✓ |
| **Clickonero ó Outlet de Viajes** | ✓ | ? | ✓ | ? | ✓ | ✗ | ✓ | ✓ |
| **Groupon ó Peixe México** | ✓ | ? | ✓ | ? | ✓ | ✗ | ✓ | ✓ |
| **Interjet** | ✓ | ? | ✓ | ? | ✓ | ✗ | ✓ | ✓ |
| **Almundo** | ✓ | ? | ✓ | ? | ✓ | ✗ | ✓ | ✓ |
| **Elektra** | ✓ | ? | ✓ | ? | ✓ | ✗ | ✓ | ✓ |
| **Cinépolis** | ✓ | ? | ✓ | ? | ✓ | ✗ | ✓ | ✓ |
| **Duran Autopartes** | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| **Proser Soluciones** | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| **Sublimarte** | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

Tabla 3.1. Apego a los principios que rigen el tratamiento de datos personales
*Fuente: Elaboración propia*

En la información contenida en la tabla anterior, se puede observar que siete de las diez empresas, cumplen en buena medida con los principios que rigen la protección de datos personales, mientras que tres de ellas no cuentan con el aviso de privacidad, esto hace que no se cumpla con el resto de los principios, a menos no existen elementos para poder evaluar su cumplimiento. Sin embargo, en lo que respecta a la proporcionalidad, ningún da de ellas demuestra que solo recolecte los datos necesarios para cumplir con las responsabilidades y obligaciones derivadas de la transacción comercial, en cuanto a los principios de lealtad y calidad, no existen elementos que puedan demostrar el cumplimiento u omisión de los mismos.

Al decir que no existen elementos, se hace referencia a que no es posible determinar si, en la práctica, los datos son tratados de manera leal y de acuerdo a las finalidades que dieron origen a su tratamiento. Por su parte, la calidad de los datos no se puede constatar mediante el aviso de privacidad, debido a que no es posible conocer si los datos recolectados se mantienen actualizados y son correctos conforme a su titular.

Lo anterior, en relación al principio de proporcionalidad, de cierta manera puede ser justificable en función de la trazabilidad de la información y el no repudio, que permite contar con los elementos necesarios de identificación, –tanto del usuario como del equipo y geolocalización–, para que no pueda darse el caso de que, quienes realicen una transacción legítima, a la postre la desconozcan pidiendo el reembolso de su dinero, de tal manera que es necesario conservar datos que ante un peritaje informático, puedan identificar plenamente al usuario que haya realizado la transacción.

No obstante, cuestiones como el seguimiento de lo que se hace en otras páginas de *Internet,* lo que se consulta en ellas, los hipervínculos a los que dé clic el usuario, es información que se sale del contexto de proporcionalidad y de la trazabilidad, llegando al grado de convertir dicha actividad en una violación a la privacidad del usuario, ello por incumplir en los principios de licitud, lealtad, consentimiento, proporcionalidad y finalidad.

Es importante resaltar que lo anterior, no es una condición recurrente por lo responsables en todas las plataformas de comercio electrónico o cómputo en la

nube, ya que para ello se requiere de tecnología para la recolección de datos, más especializada de lo que supone una plataforma de comercio electrónico, en relación a su finalidad como medio tecnológico de compra-venta. Aludiendo concretamente de empresas tecnológicas, que su principal servicio es ofertado mediante *Internet,* se entiende el interés por conocer más información de los titulares y de lo que éstos realizan en la red, para especializar los servicios que les ofrecen a sus clientes.

Casos específicos como Google y Facebook que ofrecen servicios publicitarios, pueden recolectar información de lo que los usuarios de un equipo de cómputo realizan en *Internet,* sin que la responsabilidad por esta actividad deba recaer directamente en el responsable del tratamiento de los datos, es decir, quien se presenta en el aviso de privacidad como el responsable del tratamiento de los datos, lo será solamente de aquellos datos que él recolecta para el cumplimiento de la transacción comercial y acorde a las finalidades informadas.

Sin embargo, las empresas tecnológicas señaladas, pueden recolectar mucha más información por cuenta propia como resultado del uso de sus plataformas, no como consecuencia de la transacción realizada entre el responsable de la plataforma de comercio electrónico y el titular de los datos. Por su parte, las empresas que ofrecen servicios de cómputo en la nube, pueden también hacer recolección de información adicional a la que realiza el responsable, con el objetivo de dar trazabilidad a la información y mejorar sus servicios.

Así entonces, en aras de cumplir con el principio de información y la proactividad que el reglamento europeo exige, es pertinente informar al usuario que, adicional a la información recolectada por el responsable para el cumplimiento de las finalidades previstas en el aviso de privacidad, la empresa que brinda el servicio de nube, así como la empresa propietaria del motor de búsqueda que se utilice, podrán recolectar y almacenar información del cliente con fines mercadotécnicos, actividad que no es competencia del responsable, por lo que el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, deberán ejercerse directamente ante la empresa responsable y bajo las legislaciones del país de residencia, o donde lo hayan establecido en sus condiciones de uso y/o en sus políticas de privacidad.

Por otro lado, en la tabla 3.2, se analiza si mediante el aviso de privacidad es posible identificar los elementos que den respuesta a las preguntas planteadas respecto a si, ¿Realiza transferencia internacional de datos?; ¿Realiza transferencia nacional de datos?; ¿Informa sobre seguridad implementada?; ¿Informa sobre tecnologías de recolección de datos?; ¿Establece procedimiento para el ejercicio de los derechos ARCO?; ¿Es proactivo?; ¿Uso de los datos para fines publicitarios?; ¿Separa los avisos de privacidad por destinatario?; ¿Informa sobre el tratamiento de datos sensibles? y ¿Contempla la protección de menores?.

| Empresa | Realiza transferencia internacional de datos | Realiza transferencia nacional de datos | Informa sobre seguridad implementada | Informa sobre tecnologías de recolección de datos | Establece procedimiento para el ejercicio de los derechos ARCO | Es proactivo | Uso de los datos para fines publicitarios | Contempla la protección de menores | Separa los avisos de privacidad por destinatario | Informa sobre el tratamiento de datos sensibles | Cuenta con aviso de uso de cookies |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **PriceTravel** | ✓ | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ |
| **Clickonero ó Outlet de Viajes** | ? | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ |
| **Groupon ó Peixe México** | ? | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ |
| **Interjet** | ? | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ |
| **Almundo** | ? | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ | ✓ | ✗ |
| **Elektra** | ✗ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ | ✓ |
| **Cinépolis** | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ | ✓ |
| **Duran Autopartes** | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| **Proser Soluciones** | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| **Sublimarte** | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |

Tabla 3.2. Elementos para garantizar la libre autodeterminación informativa
*Fuente: Elaboración propia*

De la tabla anterior, se puede destacar de las empresas que sí cuentan con un aviso de privacidad, el hecho de que sí informan a los usuarios de manera adecuada sobre tecnologías de recolección de información, establece un procedimiento para

ejercer los derechos ARCO e identifican el tratamiento de datos sensibles. Aunque parece que para la mayoría de las empresas, la proactividad no es una práctica de su interés, además de lo ya mencionado anteriormente respecto a la proporcionalidad de la información recolectada, el hecho de informar sobre la recolección y el tratamiento de esa información, no subsana el incumplimiento al principio de proporcionalidad en el sentido estricto de la Ley.

Asimismo, la mayoría de las empresas redactan de manera confusa las finalidades del tratamiento de los datos que recolectan, pues no separan las finalidades primarias de las secundarias. Como ejemplo, Cinépolis establece finalidades publicitarias y de prospección comercial como finalidades del tratamiento, la oposición a dichas finalidades se deberá realizar mediante solicitud al departamento de datos personales, lo cual, incumple con el principio de finalidad establecido en la Ley.

Por otro lado, los mecanismos implementados para el ejercicio de los derechos ARCO, mediante los cuales se puede oponer el titular al tratamiento de sus datos, son insuficientes, en su mayoría solo se hace mención del procedimiento y no se proporcionan guías de apoyo para su ejercicio. Esto, parece obedecer por una parte al desconocimiento de la Ley, y por otra a la falta de cultura de la proactividad, lo que deriva en múltiples violaciones por parte de los responsables[150].

### *3.2. Análisis comparativo de las Leyes de Europa y México en materia de protección de datos personales*

El análisis comparativo que se hace en este apartado, toma en cuenta la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* el *Reglamento General de Protección de Datos del Consejo de Europa* y el *Convenio 108 del Consejo de Europa*, en ellos se buscan elementos de similitud y diferencias en cuanto a los principios y mecanismos de protección del derecho en cuestión. Se comparan con la intención de determinar, cual resulta más adecuado para

[150] *Cfr.* Auren Iberoamerica, *Estudio de Cultura sobre Tratamiento de Datos Personales en el Sector de las Tecnologías de la Información,* CANIETI, Secretaría de Economía y PROSOFT 2.0, s.f., p. 70.

garantizar la salvaguarda del derecho a la protección de datos personales ante el entorno de cómputo en la nube.

En tal sentido y a manera de preámbulo, es de interés resaltar que el reglamento toma como referencia el artículo 16, apartado 2 del *Tratado de Funcionamiento de la Unión Europea*[151]*,* que encomienda al parlamento y al consejo, establecer normas de protección y a la libre circulación de los datos de carácter personal, así como en el apartado 1 donde manifiesta que "toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan"[152]. De tal manera que se ha visto la importancia del flujo de la información para el desarrollo económico, pero se ha buscado crear normativas para la protección de los derechos de la personalidad, sin limitar el flujo de información, haciendo que el tratamiento de la misma sea de manera controlada e informada.

Por otro lado, la *Carta de los Derechos Fundamentales de la Unión Europea,* en su artículo 8, relativo a la protección de datos de carácter personal, apartado 1, reconoce que "Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan"[153], y establece también, con respecto al tratamiento de los datos de carácter personal, que:

> 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
> 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente[154].

En concreto, en el documento de interés para este apartado, se observa que en el *Reglamento General de Protección de Datos del Consejo de Europa* se menciona que, "[…] El Derecho de la Unión o de los Estados miembros debe establecer

---

[151] Diario Oficial de la Unión Europea, *Versión consolidada del tratado de funcionamiento de la unión europea,* 2012, p. 9, https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12012E/TXT&from=ES. Consultado: 20/03/2020.
[152] *Idem.*
[153] Diario Oficial de las Comunidades Europeas, *Carta de los derechos fundamentales de la unión europea,* 2000, p. 10, https://www.europarl.europa.eu/charter/pdf/text_es.pdf. Consultado: 20/03/2020.
[154] *Idem.*

medidas específicas y adecuadas para proteger los derechos fundamentales y los datos personales de las personas físicas"[155]. Esto, con respecto a México, se traduce en una obligación acorde a lo establecido tanto en el *Convenio 108,* como en el citado reglamento, ya que, al ser un país firmante del convenio, debe acatar lo establecido en relación a la protección de los derechos humanos[156], para este caso, se hace énfasis en el derecho a la protección de datos personales.

No es coincidencia que México se haya adherido al *Convenio 108,* pues para que un estado pueda ser miembro de dicho convenio, debe contar con una legislación que garantice en buena medida el derecho a la protección de los datos personales, por ello se entiende que la legislación mexicana en materia de protección de datos personales, si bien, no es tan especializada como la de la Unión Europea, si se acerca a los parámetros generales de la misma, y a los principios que rigen el tratamiento de los datos personales.

No obstante, en cuanto a los principios se refiere, el *Reglamento General de Protección de Datos del Consejo de Europa* en su capítulo II, relativo a los principios, establece que los datos personales deberán ser tratados bajo los principios de: a) licitud, lealtad y transparencia; b) limitación de la finalidad; c) minimización de datos; d) exactitud; e) limitación del plazo de conservación; f) integridad y confidencialidad, además, establece también que el responsable deberá demostrar su capacidad para el tratamiento de los mismas bajo los principios mencionados, lo que se denominó como, "responsabilidad proactiva"[157].

En tal sentido, el principio de licitud, en denominación concuerda con el mismo principio de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* mientras que en descripción de lo que ello implica, la Ley antes citada dificulta la comprensión del mismo, puesto que no hace referencia claramente a el principio en cuestión, y en su contenido indica literalmente que:

> Los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por esta Ley y demás normatividad aplicable.

---

[155] *Cfr. Diario Oficial de la Unión Europea, Reglamento (UE) 2016/679…, Op. Cit. Considerando 53, pp. 10–11.*
[156] *Cfr. Ibidem,* Considerando 104, 105 y 106, pp. 19–20.
[157] *Cfr. Ibidem,* pp. 35–36

> La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.
> En todo tratamiento de datos personales, se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por esta Ley[158].

Como se puede observar, en ningún momento hace mención clara de que, para cumplir con el principio de licitud, el tratamiento debe reunir ciertas características específicas, en su lugar solo menciona que los datos deben ser tratados de manera lícita conforme a la Ley. Sin embargo, en el resto de la Ley no se aclara a que se refiere con la licitud, o que elementos deben cubrirse para considerar que el tratamiento es lícito.

Contrario a ello, en el reglamento en cuestión se dedica un apartado para describir el principio de *licitud, lealtad y transparencia,* en él se encuentran las características que debe reunir el tratamiento de los datos para cumplir con el principio de licitud, dichas características engloban el resto de los principios, por lo que se considera como un principio de suma importancia. Entre otras cuestiones, considera que el tratamiento será lícito cuando:

> 1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
> a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
> b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
> c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;
> d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
> e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;
> f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

[158] Ley Federal de Protección de Datos… *Op. Cit.* Artículo 7, p. 3.

> Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.[159]

Como se puede observar, el consentimiento es parte fundamental para el tratamiento lícito de los datos personales[160], así como, la lealtad y la transparencia, lo cual también engloba la obligación de informar al titular sobre los fines para los cuales se obtiene la información[161], de tal manera que en comparación con la legislación mexicana, el reglamento engloba en un solo principio, los principios de licitud, lealtad, consentimiento y finalidad contenidos en la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares.*

Además, los temas de licitud, lealtad y transparencia, así como el consentimiento, son abordados en varios de los considerandos con la intención de especificar los casos en que se deben considerar dichos principios, ello con la intención de servir de guía al momento del tratamiento de datos personales, esto puede variar según la finalidad y los titulares de que se trate.

Respecto al consentimiento se dedica el artículo 7, denominado “condiciones para el consentimiento”[162] y el artículo 8 denominado “condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información”[163].

Al respecto, la Ley mexicana establece en su artículo 8, que todo tratamiento requiere del consentimiento del titular, en el se hace referencia al tipo de consentimiento tácito y expreso, requiriendo para el tratamiento de datos financieros o patrimoniales, el consentimiento expreso del titular, mientras que, para tratamientos de información de identificación, solo se requiere el consentimiento tácito. De igual manera en dicho artículo, se establece que el consentimiento podrá ser revocado en cualquier momento, y que el responsable deberá establecer procedimiento para orientar al titular a realizar la revocación del consentimiento, siempre y cuando así lo permita la relación contractual.

---

[159] *Cfr.* Diario Oficial de la Unión Europea, *Reglamento (UE) 2016/679…, Op. Cit.* pp. 36–37.
[160] *Cfr. Ibidem,* Considerando 40, pp. 7–8.
[161] *Cfr. Ibidem,* Considerando 60, p. 12.
[162] *Cfr. Ibidem,* Artículo 7, p. 37.
[163] *Cfr. Idem.*

En cuanto a las excepciones que la Ley contempla como casos en los que no se requiere el consentimiento del titular, el artículo 10 menciona los supuestos en los que no será necesario el consentimiento, mientras que el artículo 37 enuncia los casos en los que las transferencias internacionales o nacionales podrán llevarse a cabo sin el consentimiento, no siendo necesario el consentimiento cuando:

> I. Esté previsto en una Ley;
> II. Los datos figuren en fuentes de acceso público;
> III. Los datos personales se sometan a un procedimiento previo de disociación;
> IV. Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;
> V. Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
> VI. Sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones jurídicas aplicables y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente, o
> VII. Se dicte resolución de autoridad competente[164].

Respecto a la disociación de los datos personales, es importante señalar que dicho procedimiento deberá imposibilitar la identificación de la persona, por ejemplo, para cuestiones estadísticas en las que, los datos personales no son tratados con la intención de identificar a la persona, sino, para contabilizarla a manera de estadística, como podría ser el caso del reporte de ventas, donde no se requiere tener más que los números de ventas, quizá el género del comprador, la nacionalidad o su localización geográfica por ciudad. Estos datos podrían ser tratados sin el consentimiento del titular, ya que el uso de los mismos no supone la identificación de la persona.

Mientras que las transferencias de datos personales podrán realizarse sin el consentimiento de los titulares:

> Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte;

[164] Ley Federal de Protección de Datos… *Op. Cit.,* Artículo 10, p. 4.

> II. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;
> III. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;
> IV. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;
> V. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;
> VI. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y
> VII. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular[165].

En relación a las transferencias, se puede resumir de manera general en que, no se requiere del consentimiento del titular cuando existe un interés general como es el caso de la salud pública, en temas de investigación de delitos y cuando las autoridades competentes así lo requieran, cuando se haga entre empresas del mismo grupo o cuando esté prevista en un tratado internacional. Al respecto, México, al haber firmado el *Convenio 108 del Consejo de Europa,* podría realizar la transferencia internacional a cualquier parte de Europa, sin el consentimiento del titular; ello no supone una violación a los derechos de la persona, más bien, supone que detrás de la adhesión a dicho convenio, existe la expectativa de que los datos serán tratados bajo condiciones adecuadas para garantizar la protección de la privacidad de las personas.

No obstante, preocupa que la Ley mexicana no contemple en ningún momento mecanismos relativos al consentimiento de datos personales de menores. Al respecto, lo único que se puede observar es lo relativo al ejercicio de los derechos ARCO que se enuncia en el reglamento de la Ley, donde se indica que ante tales casos "[…] se estará a las reglas de representación dispuestas en el *Código Civil Federal"*[166].

En cuanto al principio de *limitación de la finalidad*, este se entiende de la misma manera en que se retoma en la legislación mexicana, "recogidos con fines

[165] *Ibidem,* Artículo 37, p. 9.
[166] Reglamento de la Ley Federal de Protección de Datos…, *Op. Cit.,* Artículo 89, p. 23.

determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines […]"[167], sin contemplar como incompatible las finalidades de investigación científica e histórica, estadísticos o cuándo se trata de datos de interés público.

En relación a este principio, se ha observado que, a menudo, las empresas que recolectan datos personales lo usan para finalidades incompatibles a aquellas que dieron origen al tratamiento, por ejemplo, cuando se responde a una encuesta, el aviso de privacidad puede establecer que los datos se recolectan para fines estadísticos, pero a la postre, podemos estar recibiendo invitaciones a eventos o publicidad, algo que no es compatible con lo que se había informado en un principio, esto supone una violación a la finalidad, ya que como se infiere por la definición del principio en el reglamento europeo, la finalidad debe marcar una limitación del uso de los mismos, solo para el cumplimiento de la finalidad informada.

Respecto al principio de *minimización de los datos*, además de lo señalado en el apartado relativo a los principios, también está relacionado con la protección de datos desde el diseño y por defecto, según lo indicado en el artículo 25 del reglamento[168]. En comparación con la legislación mexicana, se observa una deficiencia ya que no contempla la protección de los datos desde el diseño y por defecto.

Por su parte el principio de exactitud, concuerda con el principio de calidad contenido en la legislación mexicana, la finalidad es que, los datos que se conservan de los titulares sean correctos y actualizados, asimismo, establece que deben adoptarse las medidas necesarias, para que éstos puedan ser rectificados o suprimidos en caso de ser inexactos, o incompatibles conforme a los fines para los que fueron recabados.

La *limitación del plazo de conservación,* es un principio que no tiene correspondencia con ninguno de los establecidos en la legislación mexicana, ya que este se retoma solamente como un elemento del principio de calidad, así como la

[167] *Cfr. Ibidem,* Artículo 5, p. 35.
[168] *Cfr. Ibidem,* Artículo 25, p. 48.

mención de un periodo de bloqueo de los datos al momento de ejercer los derechos ARCO, sin brindar más aclaraciones.

El principio de *integridad y confidencialidad,* se relaciona con los artículos 19, 20 y 21 de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* lo que sugiere que se deben implementar medidas de seguridad para evitar que la información sufra daños, pérdida o sea utilizada de manera ilícita por personas ajenas o de la misma empresa.

En un amplio sentido, se puede decir que la legislación mexicana cumple con los mismos principios que el reglamento de Europa, ya que, si se cumple con los principios establecidos en la Ley, se estaría garantizando la salvaguarda del derecho a la protección de los datos personales y la autodeterminación informativa. No obstante, el reglamento cuenta con elementos de orientación que sugieren mayor probabilidad de cumplimiento, además de contar con mayores elementos de responsabilidad por parte de los órganos garantes, ello propicia un mecanismo de ejecución más efectivo que el establecido en la Ley mexicana.

Por tanto, las deficiencias más notorias son en cuanto a las autoridades de control y su especialización, así como en los derechos de los titulares, ya que la legislación mexicana no contempla, por ejemplo, el derecho a la portabilidad, el derecho a la limitación del tratamiento, ni la necesidad de establecer mecanismos de cooperación internacional, a fin de coadyuvar en la investigación y resolución de las denuncias de los ciudadanos, incluso, para llevar a cabo inspecciones de oficio a manera de supervisión del cumplimiento de la Ley por parte de los responsables.

### *3.3. La pertinencia de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares ante el uso de la tecnología de cómputo en la nube*

En lo que respecta a la regulación del tratamiento de datos personales en la nube, a la luz de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* es evidente que aún falta camino por recorrer en aras de proteger la privacidad de las personas ante el uso de esta tecnología, como se menciona con anterioridad, las plataformas de nube suponen el uso de *Internet* para poder operar, mientras que el uso de *Internet* supone la utilización de tecnologías de terceras

empresas tecnológicas como Google, Facebook, Amazon y Apple, además de algunas otras emergentes, y de aquellas aplicaciones que se instalan con intención de recolectar información de la navegación del usuario en la red.

Estas cuestiones aun no son tomadas en cuenta de manera precisa por la Ley, siendo una deficiencia con respecto al tratamiento de datos personales, ya que al momento de usar estas tecnologías los usuarios podrían estar siendo objeto de violaciones a sus derechos humanos, mientras que la Ley no establece una limitación del tratamiento de los datos personales en torno al uso de estas tecnologías.

Cabe señalar que el detonante de las leyes en materia de protección de datos personales, fue el uso de las tecnologías para el tratamiento de datos personales de manera automatizada, esto por suponer una vulneración a la privacidad de las personas, que puede dañar su dignidad, honor, reputación y la propia imagen.

En tal sentido, analizando lo que la legislación mexicana, en materia de protección de datos personales establece con respecto al tratamiento de los datos personales en entornos de nube, no se encuentran elementos que manifiesten la necesidad de implementar mecanismos de protección, así como limitación de la recolección de datos personales en entornos tecnológicos.

En la mencionada Ley, con relación al uso de las tecnologías de comercio electrónico –las cuales suponen el uso de tecnologías de nube–, en el artículo 43, fracción VIII, se asigna a la Secretaría de Economía las atribuciones para, “diseñar e instrumentar políticas y coordinar la elaboración de estudios para la modernización y operación eficiente del comercio electrónico, así como para promover el desarrollo de la economía digital y las tecnologías de la información en materia de protección de datos personales”[169].

Sin embargo, esto no orienta a los responsables para el adecuado tratamiento de dichas tecnologías, por ende, las empresas que hacen uso de ellas, pueden violar los principios que rigen el tratamiento de los datos personales, no por intención u omisión, sino por la libertad al no haber disposiciones específicas en la

[169] Ley Federal de Protección de Datos… *Op. Cit.* Artículo 43, Fracción VIII, p. 11.

Ley, incluso por el desconocimiento o de manera consciente al no tener restricciones concretas que impidan realizar dichas acciones.

Cabe destacar que el reglamento de la citada Ley, sí reconoce el tratamiento de datos personales en el cómputo en la nube en el artículo 52. No obstante, si se analiza lo que aquí se dispone, parece incongruente lo que se establece como requisitos para el uso de servicios de cómputo en la nube, tomando en consideración la forma en que operan dichas empresas tecnológicas.

En tal sentido, las empresas que contratan los servicios de cómputo en la nube se adhieren a los contratos de las empresas tecnológicas prestadoras de dichos servicios, como son Amazon, Google, Salesforce, Microsoft o Apple, por mencionar algunas de las más grandes. Cabe señalar en tal sentido que, estas empresas no dan más información de la necesaria para la contratación del servicio, y quien quiera usar su tecnología, no tendrá opción distinta que aceptar las condiciones de su contrato de adhesión, lo que impide el cumplimiento de lo establecido en el artículo 52, en el que se lee que:

> Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor:
>
> I. Cumpla, al menos, con lo siguiente:
>
> a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y el presente Reglamento;
>
> b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;
>
> c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio;
>
> d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio, y.
>
> II. Cuente con mecanismos, al menos, para:
>
> a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;
>
> b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;
>
> c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio;
>
> d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y

> e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.
>
> En cualquier caso, el responsable no podrá adherirse a servicios que no garanticen la debida protección de los datos personales.
>
> Para fines del presente Reglamento, por cómputo en la nube se entenderá al modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o software, que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente.
>
> Las dependencias reguladoras, en el ámbito de sus competencias, en coadyuvancia con el Instituto, emitirán criterios para el debido tratamiento de datos personales en el denominado cómputo en la nube[170].

Como se observa en tales disposiciones y en relación a lo analizado respecto al funcionamiento de las tecnologías, no sería posible hacer uso de estas tecnologías por la manera en la que operan, así como por la dificultad que las empresas puedan tener para que el proveedor del servicio pueda demostrar lo que se establece en la Ley, ya que algunos de los elementos que se pide demostrar, podrían poner en riesgo la seguridad de la información, motivo por el cual no será posible que se cumpla con la Ley en tal sentido.

Así entonces, hace falta que la ley establezca mecanismos de limitación de la recogida de datos, no solo para las empresas responsables, sino a nivel global para las empresas tecnológicas, que explotan de manera desproporcionada los datos personales en beneficio de sus servicios publicitarios[171], que resultan violatorios de derechos humanos.

Por lo anterior, en cuanto a la pertinencia de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* como la norma creada para garantizar la protección de datos personales, incluyendo entornos de cómputo en la nube, se puede decir que aún queda camino por recorrer para lograr la armonización entre tecnología y derechos humanos.

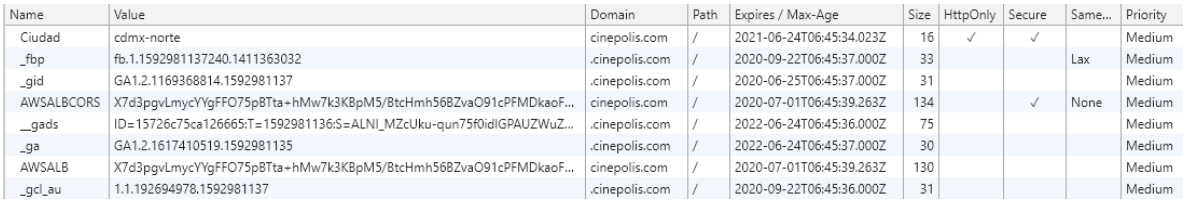
A manera de ejemplo respecto al uso de tecnologías, podemos observar que al momento de ingresar a la página de www.cinepolis.com.mx, si revisamos las

---

[170] *Ibidem,* pp. 13–14.

[171] Comisión Europea, *Antimonopolio: La Comisión impone a Google una multa de cerca de 4,34 miles de millones EUR por prácticas ilegales en relación con los dispositivos móviles Android para reforzar la posición dominante del motor de búsqueda de Google,* 2018, [en línea], https://ec.europa.eu/commission/presscorner/detail/es/IP_18_4581. Consultado: 20/01/2020.

cookies que se cargan, localizamos ocho, de las cuales se desconoce a ciencia cierta qué es lo que permiten recolectar del navegador del usuario, tal como se observa en la figura 3.1.



| Name | Value | Domain | Path | Expires / Max-Age | Size | HttpOnly | Secure | Same... | Priority |
|---|---|---|---|---|---|---|---|---|---|
| Ciudad | cdmx-norte | cinepolis.com | / | 2021-06-24T06:45:34.023Z | 16 | ✓ | ✓ | | Medium |
| _fbp | fb.1.1592981137240.1411363032 | .cinepolis.com | / | 2020-09-22T06:45:37.000Z | 33 | | | Lax | Medium |
| _gid | GA1.2.1169368814.1592981137 | .cinepolis.com | / | 2020-06-25T06:45:37.000Z | 31 | | | | Medium |
| AWSALBCORS | X7d3pgvLmycYYgFFO75pBTta+hMw7k3KBpM5/BtcHmh56BZvaO91cPFMDkaoF... | cinepolis.com | / | 2020-07-01T06:45:39.263Z | 134 | | ✓ | None | Medium |
| __gads | ID=15726c75ca126665:T=1592981136:S=ALNI_MZcUku-qun75f0idlGPAUZWuZ... | .cinepolis.com | / | 2022-06-24T06:45:36.000Z | 75 | | | | Medium |
| _ga | GA1.2.1617410519.1592981135 | .cinepolis.com | / | 2022-06-24T06:45:37.000Z | 30 | | | | Medium |
| AWSALB | X7d3pgvLmycYYgFFO75pBTta+hMw7k3KBpM5/BtcHmh56BZvaO91cPFMDkaoF... | cinepolis.com | / | 2020-07-01T06:45:39.263Z | 130 | | | | Medium |
| _gcl_au | 1.1.192694978.1592981137 | .cinepolis.com | / | 2020-09-22T06:45:36.000Z | 31 | | | | Medium |

Figura 3.1. Cookies cargadas en el portal de internet de www.cinepolis.com
*Fuente: Captura de pantalla del navegador Google Chrome*

Estos archivos que se muestran en la imagen anterior, pueden estar recolectando información mediante código, que puede ser JavaScript, Vue.js, React.js o alguna otra variante de programación web que permita la recolección de los datos concernientes a la actividad que el usuario realiza en *Internet.* Posteriormente, se puede acceder a este archivo y leer los datos que se hayan recolectado.

Si bien, las cookies no son archivos maliciosos ni permiten la inyección de virus por terceros e incluso la función más común de las cookies es guardar los valores de identificación de una página web para que la siguiente vez que esta sea accedida, el tiempo de respuesta sea más rápido, también existen las cookies conocidas como tracking cookies o cookies de seguimiento, las cuales se programan con la intención de dar un seguimiento a la actividad del usuario en *Internet.*

Es importante también señalar que no se usan para recolectar datos como nombre, domicilio, teléfono u algún otro dato inherente a la persona, motivo por el cual se cree que el uso de las mismas no vulnera el derecho de los titulares. Sin embargo, si pueden recolectar datos como la dirección IP, la geolocalización, la sesión del navegador al ingresar a la página, así como las pestañas a las que da clic el usuario, en algunos casos desde la página anterior a ingresar a esta página y la que se visite después de abandonar dicha página web.

El ejemplo de dicho rastreo se encuentra en el aviso de privacidad de Pricetravel, que en el punto 4.1, menciona que usa cookies y Web Beacons para obtener información como: “Su tipo de navegador y sistema operativo; Las páginas de

*Internet* que visita; Los vínculos que sigue; La dirección IP y el sitio que visitó antes de entrar al nuestro”[172].

Como ejemplo de otras cookies que se conocen como de personalización, se puede observar en el ejemplo anterior referente a Cinépolis; la primera de las cookies que se visualiza en la Figura 3.1, se llama ciudad, esto, en concordancia con el aviso de privacidad, sirve para personalizar la ciudad, es decir que el usuario, al consultar la cartelera, debe seleccionar una ciudad, pero la próxima vez que consulte la cartelera, ya no será necesario volver a seleccionar la ciudad, pues este dato permanece en la cookie de personalización y reconoce que el usuario ya ha seleccionado la ciudad anteriormente y se sobre entiende, que el usuario que usa ese mismo dispositivo, permanece en la misma ciudad.

Parece irrelevante pero en la era de la información, esto ayuda a que los usuarios se sientan atendidos por las empresas, hace parecer que realmente les importa la comodidad y que se preocupan por ellos, aunque realmente tenga una finalidad mercadotécnica, además de servir como datos estadísticos, amén de que, al concatenar esta información con otros datos que pueden estar siendo recolectados por las múltiples cookies que se ejecutan, pueden dar origen a la identificación de la persona, así como de sus gustos, actividad que se sale de los parámetros establecidos en los principios que rigen el tratamiento de los datos personales.

En ese sentido, la Ley se debe adecuar para garantizar la protección de los derechos humanos ante el uso de las tecnologías. No obstante, respecto a los principios, en general, se puede afirmar que la Ley mexicana cumple con los requerimientos generales de la protección de los datos personales, aunque, en comparación con el reglamento europeo, queda corta en descripción de lo que se debe hacer tanto por los responsables como por las autoridades reguladoras, las facultades y la autonomía de las mismas para la imposición de sanciones.

[172] Price Travel. *Aviso de privacidad.* https://www.pricetravel.com/info/aviso-privacidad

*3.4. Protocolos de comunicación y sus posibles vulneraciones a la privacidad*

Otro factor a tener en cuenta en el tratamiento de los datos personales en sistemas de cómputo en la nube y en las transacciones del comercio electrónico, además de las ya mencionadas anteriormente, es la tecnología de comunicación, en concreto, los protocolos de comunicación de transferencia de hipertexto HTTP *(Hypertext Transfer Protocol, por sus siglas en inglés)* y el Sistema de nombres de dominio DNS *(Domain Name System, por sus siglas en inglés).*

Lo anterior, deriva del interés de los responsables, establecido en el considerando 49 del *Reglamento General de Protección de Datos del Consejo de Europa*, donde se establece que el responsable debe "[…] garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema de información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos […]"[173] a través de las redes.

En ese sentido, podríamos analizar en su totalidad la función de cada una de las capas de la arquitectura de comunicación TCP/IP. Sin embargo, resulta muy extenso para el tema en cuestión, por ello, solo se mencionará a grandes rasgos la separación de cada capa, para después abordar solo dos de los protocolos de la capa de aplicación, HTTP y DNS, por su relevancia en el tratamiento de los datos personales y la privacidad.

Dicho lo anterior, la arquitectura TCP/IP se divido en: capa de aplicación, en la cual se ejecutan los protocolos que permiten la comunicación entre las capas inferiores para poder estructurar y transportar las consultas del usuario en *Internet,* y poder visualizarlas o interpretarlas en el otro extremo, en esta capa se ejecutan protocolos para el envío de correo electrónico, acceso a contenido web y transferencia de archivos[174].

Por su parte, la capa de transporte, es la encargada de gestionar la comunicación con la aplicación, así como de acusar el recibo de los paquetes y dar secuencia a

[173] *Cfr.* Diario Oficial de la Unión Europea, *Reglamento (UE) 2016/679…,* Considerando 49, *Op. Cit.* p. 9.
[174] *Cfr.* Kenneth C., Laudon y Guercio Traver, Carol, *E-commerce 2013. Negocios…* Op. Cit. p. 1124.

los mismos para enviarlos a la capa de aplicación para la visualización en pantalla[175].

La capa de *Internet,* es la responsable de empaquetar y enrutar los paquetes hacia *Internet,* mientras que la capa de red es la encargada de enviar y recibir los paquetes en forma de 0s y 1s, para que estos puedan viajar mediante pulsos electromagnéticos, y al recibirlos, los delega a las capas superiores para su desempaquetado e interpretación[176].

Así entonces, debemos tener en cuenta que, para poder acceder a un servicio en línea, se requiere de un navegador web, es decir un software que permita acceder al contenido que se encuentra almacenado en algún servidor web. Este software, debe ejecutar una serie de protocolos para poder mostrar el resultado en pantalla al usuario.

Ahora bien, ¿cómo opera el protocolo HTTP?, su operación, para un mejor entendimiento, se puede simplificar en dos pasos, primero, el navegador manda una petición de tipo HTTP solicitando un archivo, el servidor que contiene el archivo solicitado, responde al navegador con la información y este la interpreta para mostrarla al usuario, todo ello gracias al protocolo HTTP.

En este proceso lo que debemos tener en cuenta es que, al momento de establecer una conexión entre el navegador y el servidor, se crea una sesión, la cual dependiendo del contenido solicitado podría iniciar más de una sesión, esta se representa en un código token, que identifica al equipo que está consumiendo los datos del servidor. El problema que se podría presentar aquí, es que un intruso se robe la sesión para autenticarse y continuar con la transferencia de información entre el servidor y el intruso.

Otro problema que se puede presentar es, que si en la empresa no se ha implementado una política de seguridad adecuada y un intruso vulnera la seguridad de la red, podría perpetrar un ataque de tipo *sniffer* para obtener nombres de usuario y contraseñas de acceso a los servicios de nube, donde se almacenan los datos

[175] *Cfr. Idem.*
[176] *Cfr. Idem.*

personales, lo que permitiría tener control de los mismos sin la autorización del responsable.

A manera de ejemplo de un ataque de tipo *sniffer,* se presenta la figura 3.2 para ejemplo de captura de tráfico con el software *Wireshark,* en el cual se captura el tráfico de la red al momento de acceder al servicio del Sistema Integral de Información Administrativa (SIIA), de la Universidad Michoacana de San Nicolás de Hidalgo, se ingresa al panel de alumnos mediante usuario y contraseña. Al analizar el tráfico HTTP, en el método GET se puede localizar el usuario y la contraseña, lo cual, analizado desde un entorno de producción, donde el acceso fue realizado al sistema que almacena la información de los alumnos, le dará al atacante la posibilidad de extraer la información haciéndose pasar por un usuario auténtico, además de localizar también la sesión que podría usar para establecer una sesión en el servidor, usurpando al usuario real.

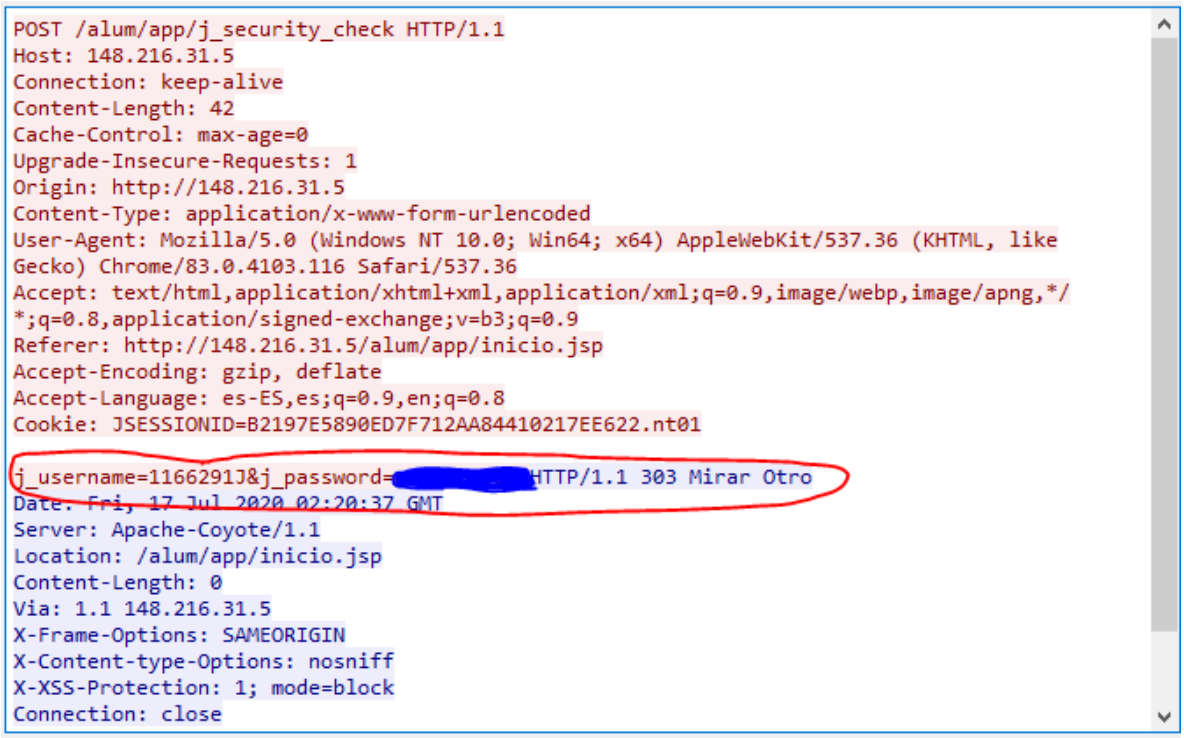



Figura 3.2. Obtención de usuario y contraseña mediante Wireshark
*Fuente: Elaboración propia*

*3.4.1. DNS y posibles vulneraciones a la privacidad*

En este apartado se pretende explicar que es el DNS, su función, la manera en que opera y como podría esta tecnología vulnerar el derecho a la protección de datos personales. Además, es importante señalar que se relaciona con la nube debido a que cualquier consulta DNS, recae en un host que se encuentra ubicado en algún lugar desconocido y que puede almacenar sistemas en los que se tratan datos personales.

Así entonces, DNS corresponde al acrónimo en inglés del protocolo llamado *Domain Name System* que, traducido al español, se entiende como el Sistema de Nombres de Dominio, es decir el protocolo que los proveedores de nombres de dominio deben seguir para poder prestar el servicio de registro de nombres de dominio y los estándares técnicos que se deben cumplir, todo esto se puede observar en los *Request for Comments (RFC)* 1034[177] y 1035[178] redactados en el año 1987 por el *Information Sciences Institute (ISI)* de la *University of Southern California.*

Al hablar de un protocolo, se hace referencia a un conjunto de procedimientos que se deben cumplir para poder identificar de alguna manera, todos los servidores que pueden almacenar información sobre los equipos o servidores que almacenan contenido web, de tal manera que cuando se desee acceder a una página web, exista la infraestructura y los procedimientos que permitan localizar cualquier contenido que exista en la red, siempre y cuando se haya registrado algún nombre de dominio en alguno de los servidores autoritativos que forman parte del árbol de servidores DNS.

Para que lo anterior sea posible, el protocolo DNS establece la estructura de los servidores DNS, es decir de los equipos que deben llevar el registro de todos los sitios web, esta estructura comienza con los llamados servidores raíz o DNS raíz, los servidores DNS de nivel superior, los servidores DNS autoritativos, los servidores DNS resolver, y por último, los servidores de contenido *web* o *host.*

---

[177] *Cfr.* IETF. *Domain Names - Concepts and Facilities.* 1987. https://www.ietf.org/rfc/rfc1034.txt. Consultado: 20/04/2020.

[178] *Cfr.* IETF. *Domain Names - Implementation and Specification.* 1987. https://www.ietf.org/rfc/rfc1035.txt. Consultado: 20/04/2020.

Antes de explicar la función de los servidores DNS raíz, es de interés señalar que en un principio solo existían trece servidores de este tipo, los cuales se localizan en distintas partes del mundo y son administrados por doce empresas, privadas y gubernamentales. En la actualidad estas doce empresas han puesto en marcha más servidores, con la intención de dar respuesta a la gran demanda de la red, sin saturar los equipos que se encargan de responder a las consultas de DNS de todos los usuarios de *Internet.*

Estos servidores DNS raíz, tienen la función de mantener actualizadas las bases de datos de los servidores de nivel superior o servidores de zona, los cuales se separan por su extensión, en donde encontramos las zonas .com, .mx, .net, etc. Lo que significa que, los servidores de nivel superior se encargan de categorizar las bases de datos de los nombres de dominio según su zona, para que cuando se realice una consulta, esta se envíe por el servidor raíz a la zona correspondiente, para que esta a su vez, dirija a los servidores autoritativos correspondientes que almacenan las bases de datos de las IP públicas de los servidores de contenido, mejor conocidos como *host.*

Dicho lo anterior, se entiende que los servidores de nivel superior, categorizan las bases de datos por zona, las cuales van de la A a la M, cada una de las letras corresponde a una de las doce empresas propietarias de estos servidores, cabe señalar que VeriSign, Inc, es propietaria de dos de los servidores. De tal manera que, cuando llega una solicitud a cualquiera de los servidores raíz, puede ser atendida por alguno de los servidores de estas empresas, según la distribución geográfica y los algoritmos usados por los DNS resolver locales, y así, los servidores raíz sabrán a que servidor autoritativo dirigir la solicitud, para que entregue la información correspondiente al *host* que almacena la información consultada.

La distribución geográfica donde se encuentran estos servidores se puede consultar en la página oficial https://root-servers.org/, donde se puede observar que, al día de hoy, las empresas cuentan con presencia de servidores en el siguiente número de localizaciones, mismos que pueden ser consultados en el sitio mencionado anteriormente: A corresponde a *Verisign, Inc.,* con presencia en 43 sitios; B corresponde al *Information Sciences Institute,* presente en 6 sitios;

Corresponde al *Cogent Communications,* con presencia en 10 sitios; D corresponde a la *University of Maryland,* con presencia en 156 sitios; E el más extenso que corresponde a la *NASA Ames Research Center,* presente en 308 sitios; F corresponde al *Internet Systems Consortium, Inc.,* presente en 252 sitios; G esta corresponde a la *Defense Information Systems Agency,* con ubicaciones en 6 sitios; H pertenece a *U.S. Army Research Lab,* con presencia en 8 sitios; I corresponde a *Netnod,* presente en 72 sitios; J de nuevo esta corresponde a *Verisign, Inc.* presente en 185 sitios; K corresponde a *RIPE NCC,* con ubicaciones en 78 sitios; L corresponde a *ICANN,* con presencia en 165 sitios y por último la M que corresponde a *WIDE Project,* con presencia en 9 sitios[179].

Todos estos servidores se distribuyen geográfica y estratégicamente en las localizaciones marcadas en el mapa que se presenta en la figura 3.3, destacando que, en cada punto marcado en el mapa, se localiza la cantidad de servidores raíz que indica el número en la marca del mapa. Desde este sitio se puede hacer un acercamiento hasta localizar la letra que identifica a la empresa propietaria, de acuerdo a lo señalado anteriormente, la ubicación específica del servidor, así como conocer la dirección IP tanto versión 4 como la versión 6.


Figura 3.3. Distribución geográfica de los servidores DNS raíz
*Fuente: https://root-servers.org/*

[179] Root-servers.org. https://root-servers.org/. Consultado: 20/04/2020.

Por su parte, el servidor DNS autoritativo, cuenta con los nombres de dominio registrados y almacena también las referencias a *host,* donde se encuentra el contenido relacionado con cada uno de los nombres de dominio. No obstante, el camino para llegar al contenido consultado no siempre tiene que ser tan largo, esto lo resuelven los registros que se almacenan en la memoria caché de la computadora del usuario y/o de los servidores de resolución de nombres de dominio o resolver, pues una vez que se ha consultado un sitio web, se almacena temporalmente un registro con las credenciales de acceso al *host* que almacena el contenido.

Pensando en que, se trata de un sitio web al que se accede por primera vez, cuando el usuario teclea la dirección URL, lo primero que hace el equipo del usuario es enviar una consulta al DNS resolver, –el cual, si no se ha configurado, corresponde al servidor del proveedor del servicio de *Internet* (ISP)–, en dicha consulta se le pregunta por la identificación del *host* que almacena la página *web* buscada. Si alguien ya había consultado anteriormente este sitio, debe estar cargada la información del *host* en la caché del resolver, por lo que no será necesario consultar a algún servidor DNS raíz, en este caso, el resolver le entrega al equipo del usuario las credenciales de identificación del *host*, para que este a su vez, establezca una conexión directa y pueda realizar el intercambio de información.

Por el contrario, si el resolver no cuenta con información relacionada con el sitio consultado, debe ir a preguntar a los servidores DNS raíz sobre el sitio que se desea consultar, pero como la función de estos servidores no es la de almacenar dicha información, lo que hará es pasarle al resolver los datos de los servidores de nivel superior o de zona. Sin embargo, como la función de estos tampoco es almacenar la información del host que almacena el contenido, le devolverá al resolver los datos del servidor autoritativo que es el encargado de almacenar la información que se está buscando.

Al momento de que el DNS autoritativo le entrega al resolver las credenciales de identificación del host que almacena el contenido, el resolver se las entrega al usuario, para que este a su vez, establezca la conexión con el host y se inicie el intercambio de información.

Así, la próxima vez que el usuario quiera acceder a dicho sitio web, se establecerá la conexión sin tener que ir a preguntar al resolver, esto es gracias a la información que se encuentra almacenada en la memoria caché del equipo del usuario. Es importante señalar que esta información no se almacena de manera permanente, por lo que en algún momento será necesario volver a realizar el mismo procedimiento, aunque si el sitio está siendo visitado por varios usuarios de manera frecuente, seguramente el resolver siempre contará con las credenciales de identificación para evitar hacer uso de los servidores raíz y prolongar el tiempo de respuesta a la consulta realizada.

El procedimiento que se describe en los párrafos anteriores, se ilustra de manera gráfica en la figura 3.4, la cual muestra el flujo de la información de las consultas entre los distintos servidores, iniciando con la consulta de un usuario a la dirección www.example.com, hasta que el resolver le entrega la información necesaria para establecer la conexión. Esto, bajo el supuesto de que el usuario está consultando un nombre de dominio nuevo, del que aún no tiene conocimiento el resolver de su proveedor de *Internet* y suponiendo de que no se hayan modificado los DNS en la configuración de red de la computadora del usuario.

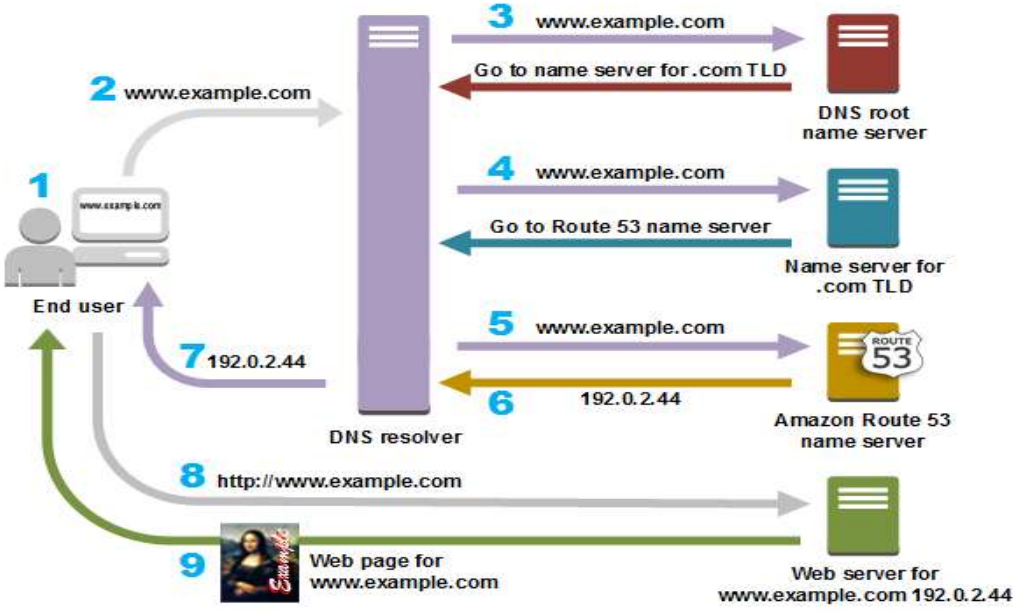



Figura 3.4. ¿De qué manera un DNS dirige tráfico hacia su aplicación web?
*Fuente: https://aws.amazon.com/es/route53/what-is-dns/*

En líneas anteriores se describió el procedimiento de la consulta, indicando que el DNS resolver pertenece al proveedor de *Internet.* Sin embargo, esto puede ser modificado al momento de configurar la dirección IP local del equipo de cómputo, de tal manera que, se puede forzar a que el DNS resolver sea un equipo propietario si se cuenta con la infraestructura, o un equipo de alguna otra empresa que ofrezca este servicio.

Existen varios DNS públicos como el de Google que es 8.8.8.8, el de IBM es 9.9.9.9 o CloudFlare 1.1.1.1, así al configurar el equipo con estos DNS, serán los servidores de estas empresas los que fungen como DNS resolver, de cierta manera, al usar estos DNS se agilizan las consultas a las páginas web, pues al ser empresas que indexan grandes cantidades de sitios, no será necesario consultar los servidores raíz para poder localizar el contenido buscado en la red.

Pero, ¿Qué ganan estas empresas por ofrecer este tipo de servicios de manera gratuita?, la respuesta es muy sencilla bajo la teoría de que nada es gratis, retomando a Jaron Lanier[180], nosotros somos el producto, no los usuarios, es decir, al navegar en *Internet* dejamos un rastro de lo que buscamos en *Internet* y le decimos a estos servidores qué es lo que consultamos, a su vez, ayudamos a que estos servidores indexen mayor cantidad de portales web, lo que incrementa el tráfico de datos hacia ellos, haciendo más prometedor el servicio de publicidad que estas empresas ofrecen a todo el que esté dispuesto a pagar por su servicio.

Ahora bien, después de saber que es el DNS y como opera, es momento de reflexionar sobre los riesgos que esta tecnología implica para la privacidad. Para ello, recordemos entonces que las Leyes de protección de datos personales han establecido los principios que rigen el tratamiento de los datos personales, entre ellos, interesa mayormente en este apartado, el principio de proporcionalidad, de información y el de consentimiento, pues cuando navegamos en *Internet,* estamos dejando un rastro que es aprovechado por las grandes tecnológicas que controlan los DNS.

---

[180] *Cfr.* Lanier, J. *Diez razones para borrar tus redes sociales de inmediato,* Barcelona, España, 2018, pp. 19–20.

Con ello pueden saber qué es lo que estamos consultando, generar un perfil de los usuarios y revelar aspectos íntimos de nuestra persona sin el consentimiento del titular de esos datos –principio de consentimiento–, la recolección es realmente desproporcional al servicio que se solicita al servidor –principio de proporcionalidad–, que consiste en preguntar por la ubicación de un host determinado, todo esto sin darle a conocer claramente al cliente sobre tales acciones –principio de información–.

El punto crítico en este caso, es que la Ley no establece responsabilidades para las empresas propietarias de los DNS resolver en torno a la privacidad de los datos que recolectan, dejando la responsabilidad en manos de la empresa propietaria del portal web al que se le entregan los datos. Sin embargo, aunque dicha empresa haga lo necesario para salvaguardar la privacidad de los datos de su cliente, al momento de realizar las consultas interviene un tercero que es el servidor DNS, por lo regular, estos servidores usan el protocolo UDP para la trasferencia de los datos de la consulta, el cual no cuenta con ningún tipo de cifrado, además de que puede recolectar datos sobre los sitios consultado sin ninguna responsabilidad ante la Ley.

Si bien, este tipo de servidores no conserva datos que identifiquen a la persona, si conserva perfiles de navegación de los usuarios en la red, este puede estar identificado por medio de la dirección IP física de la computadora que realiza las consultas, este dato, concatenado con otros datos que pueden recolectar las empresas propietarias de portales web dedicados al análisis de datos de la red, puede dar origen a la identificación de la persona, todo ello derivado de las nulas restricciones de la Ley para las empresas que prestan el servicio DNS.

Si a esto se le suman los problemas que implica el que los servidores de contenido o host no usen cifrado de las consultas que se realizan en *Internet,* el tráfico de la red al momento de establecer la conexión con el servidor de contenidos, podría estar siendo interceptado por terceros ajenos a la interacción consciente del usuario, manipulando las respuestas de DNS para redirigir a otros sitios falsos destinados a robar información o suplemente para recolectar información de interés, usando métodos como el de hombre en medio o envenenamiento de memoria caché de los servidores resolver.

Cabe destacar que desde 1997 se ha venido trabajando para mejorar la seguridad del protocolo DNS, así es como nace DNSSEC[181] concebido en el RFC 2065 y descrito en 1999 en el RFC 2535, que no es más que una extensión de seguridad para DNS, con la intención de hacerlo resistente a los ataques más comunes, tales como envenenamiento de caché, ataques de denegación de servicio (DoS) y ataques de hombre en medio.

No obstante, la seguridad de la privacidad de las consultas sigue siendo una preocupación, puesto que estas siguen viajando en texto llano, permitiendo que los servidores puedan conocer los hábitos de consulta en la red, y usen esta información para fines mercadotécnicos o permitan que otras empresas hagan uso de dichos datos.

En agosto de 2015, el *Internet Engineering Task Force (IETF),* publicó el RFC 7626[182] denominado DNS *Privacy Considerations,* el cual presenta una serie de consideraciones relativas a la seguridad en las consultas DNS, y menciona que aun cuando se use el protocolo DNSSEC, puede existir una comunicación cifrada por https, pero las consultas DNS siguen siendo claras para los servidores que intervienen en el envío y respuesta de la consulta.

Estos problemas parecen resolverse con lo establecido en el RFC 7858[183] que se publicó en 2016, el cual incluye las especificaciones para que las consultas DNS cuenten con una capa de seguridad conocida en inglés como *Trasport Layer Security (TLS)* o capa de seguridad de trasporte, con ello se pretende que las consultas puedan viajar cifradas para proteger la privacidad de los usuarios, en atención a lo descrito en el RFC 7626.

Por último, en 2018 se publicó el RFC 8484[184] para definir el protocolo de consultas DNS sobre HTTPS (DoH), se dice que este protocolo cifra las consultas DNS y requiere la autenticación del servidor, esto lo hace más resistente a ataques,

---

[181] *Cfr.* INCIBE. *Estudio del Estado de DNSSEC en España.* 2018. https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/incibe_estudio_del_estado_de_dnssec_en_espana_0.pdf. Consultado: 15/05/2020.

[182] *Cfr.* IETF. *DNS Privacy Considerations.* 2015. https://www.rfc-editor.org/rfc/rfc7626.txt

[183] *Cfr.* IETF. *Specification for DNS over Transport Layer Security (TLS).* 2016. https://tools.ietf.org/html/rfc7858. Consultado: 15/05/2020.

[184] *Cfr.* IETF. *DNS Queries over HTTPS (DoH).* 2018. https://tools.ietf.org/html/rfc8484. Consultado: 15/05/2020.

pero no proporciona integridad en la respuesta por DNSSEC. Otro de los problemas, es que aún se encuentra en fase de implementación y no todos los servidores autoritativos y/o resolver usan este tipo de cifrado para las consultas DNS, por tanto, solo mitiga la vigilancia pasiva al no permitir que terceros se hagan pasar por el servicio auténtico, pero no logra ofrecer una seguridad completa que garantice la privacidad de las consultas de *Internet.*

Derivado de la aún deficiente protección de la privacidad en las consultas DNS, la Agencia Española de Protección de Datos, ha realizado un estudio sobre la privacidad en DNS, en donde presenta el siguiente resumen ejecutivo:

> El acceso a Internet, tanto desde smartphones como equipos de escritorio, utiliza servicios para facilitar el acceso a los sitios web de una forma que resulte trasparente y cómoda al usuario. Dichos servicios, conocidos como protocolo DNS, implican el tratamiento de datos por terceros distintos de aquellos que proporcionan los servicios a los que queremos acceder. Este tratamiento podría desvelar hábitos de navegación e información de geolocalización, permite generar perfiles y ser conservados de forma indefinida y existe un riesgo serio para la privacidad de los usuarios.
>
> A pesar del aumento de la concienciación sobre la privacidad en Internet, el protocolo DNS es probablemente el gran olvidado. Esta nota identifica los problemas de privacidad que puede generar el uso del protocolo DNS y las implicaciones que podría tener el tratamiento ilegítimo de esos datos. A su vez, identifica las garantías que se pueden implementar para gestionar estos riesgos tanto para los usuarios como para los proveedores de servicios en entornos domésticos y profesionales[185].

Es notorio que existe preocupación respecto a la privacidad en *Internet* y que ya se han detectado las fallas de seguridad en el protocolo DNS, así lo demuestra este tipo de estudios y algunos otros realizados por empresas de seguridad informática. Sin embargo, en el caso concreto de México, la Ley mexicana no contempla requisitos en cuanto a la resolución de consultas que el usuario realice en *Internet,* aunado a ello, las Secretaría de Economía, encargada de realizar estudios y proporcionar guías para el cumplimiento de la Ley, tampoco ha realizado estudios inherentes a la privacidad en *Internet,* y que decir del órgano garante –INAI– que

[185] Agencia española de Protección de Datos. *Privacidad en DNS.* 2019. p. 2. https://www.aepd.es/sites/default/files/2019-12/nota-tecnica-privacidad-dns.pdf. Consultado: 20/04/2020.

tampoco ha presentado estudios relacionados a los riesgos de la privacidad en las consultas DNS.

Lo anterior se concreta a la preocupación sobre el análisis de la información que se recolecta por los servidores DNS al realizar consultas en *Internet,* pues esta información viaja de un país a otro dejando un rastro que puede ser analizado por terceros o por las mismas empresas propietarias de los servidores, dando a conocer, las palabras de la búsqueda del usuario y/o generando información relacionada a la persona para usarse en campañas publicitarias sin el consentimiento del titular.

A simple vista esto no parece vulnerar los derechos de los titulares, a no ser que pensemos en una situación hipotética, en donde el usuario realice una consulta desde un buscador y en la consulta escriba literalmente la pregunta, ¿cómo decirle a mis padres que soy homosexual?, este dato corresponde a la esfera íntima de la persona, pero si el buscador no usa una capa de cifrado, el texto de la consulta viajará por la red de manera clara, permitiendo que se analice y se concatene con otros datos para inferir que el usuario es homosexual.

Lo mismo sucede cuando se realizan búsquedas sobre la posible cura o sobre qué hacer si tengo tal enfermedad, esto resulta muy valioso para las aseguradoras, pues una vez que sepan que una persona tiene una enfermedad o es propensa, la póliza tendrá un costo más elevado por la probabilidad del uso de la misma por el cliente.

Veamos entonces un ejemplo práctico del supuesto anterior en la figura 3.5, para ello, se usó un navegador de *Internet* para acceder a un sitio web, y mediante el software *WireShark* se capturó el tráfico de las consultas y respuestas DNS del usuario, con ello se pretende dejar prueba de que aun cuando pensamos que, navegar en *Internet* no deja rastro de quienes somos, en realidad no es así, pues al conocer la dirección IP física del equipo, se puede relacionar con el usuario, llegando a identificar a las personas, razón por la cual se considera que esta dirección conocida como dirección MAC *(Media Access Control)*, es un dato personal que debe ser protegido para garantizar la privacidad el usuario.


Figura 3.5. Análisis de trafico de red en una consulta DNS
*Fuente: Elaboración propia*

Si se continua con el análisis de tráfico de la red, de acuerdo a la figura 3.6 también se puede localizar información como la fecha y hora de la consulta, el país desde donde se realiza, la dirección IP física del equipo, entre otros datos que, si se analizan conjuntamente con otros servicios consultados y/o transferencias de datos, inicios de sesión en servicios de *Internet.* Pueden dar origen a la identificación de la persona.

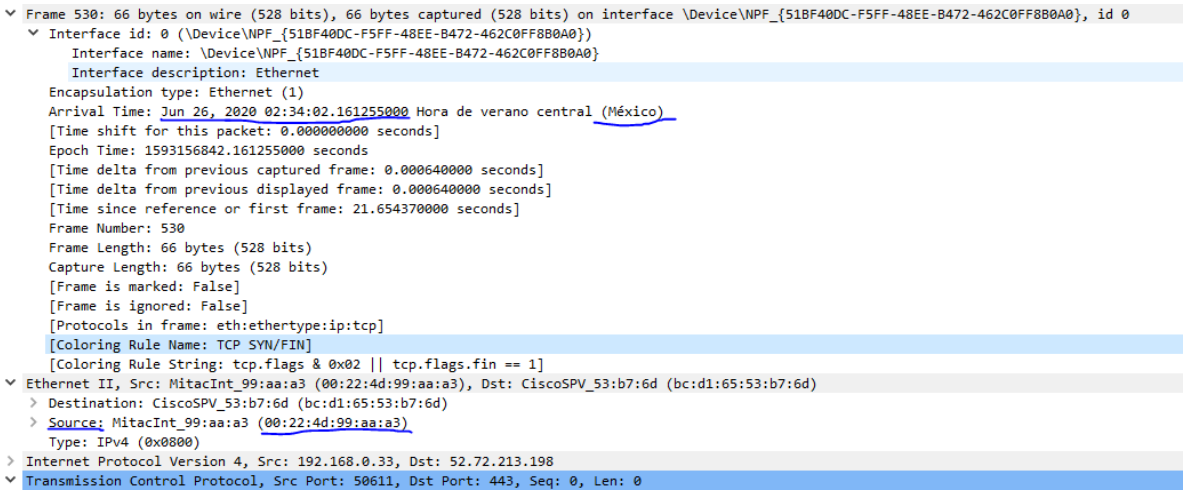



Figura 3.6. Datos de identificación del origen de la consulta DNS
*Fuente: Elaboración propia*

Si se usa Google para realizar alguna búsqueda, es posible saber a qué sitios se accedió después y cuál es el contenido visitado, e incluso se pueden recuperar las imágenes junto con otros tantos archivos sobre el contenido que se visualiza, de esta manera se puede hacer un seguimiento de los enlaces visitados para conocer sus intereses y perfilar a los usuarios. Para muestra véase la figura 3.7 que se presenta a continuación, la cual pertenece a la captura de pantalla de tráfico de red HTTP, resultado de buscar en Google el texto, “como hackear una red wifi”, y de la visita del primer enlace mostrado como resultado de dicha búsqueda

Posteriormente se hace el filtrado de paquetes HTTP y se analiza en busca de la palabra hackear con la herramienta HTTP Stream, dando como resultado el contenido de la página web visitada. De igual manera se exportan los objetos HTTP, donde se pueden visualizar las imágenes contenidas en este sitio web consultado, lo que resulta bastante delicado cuando hablamos de la privacidad en la red.

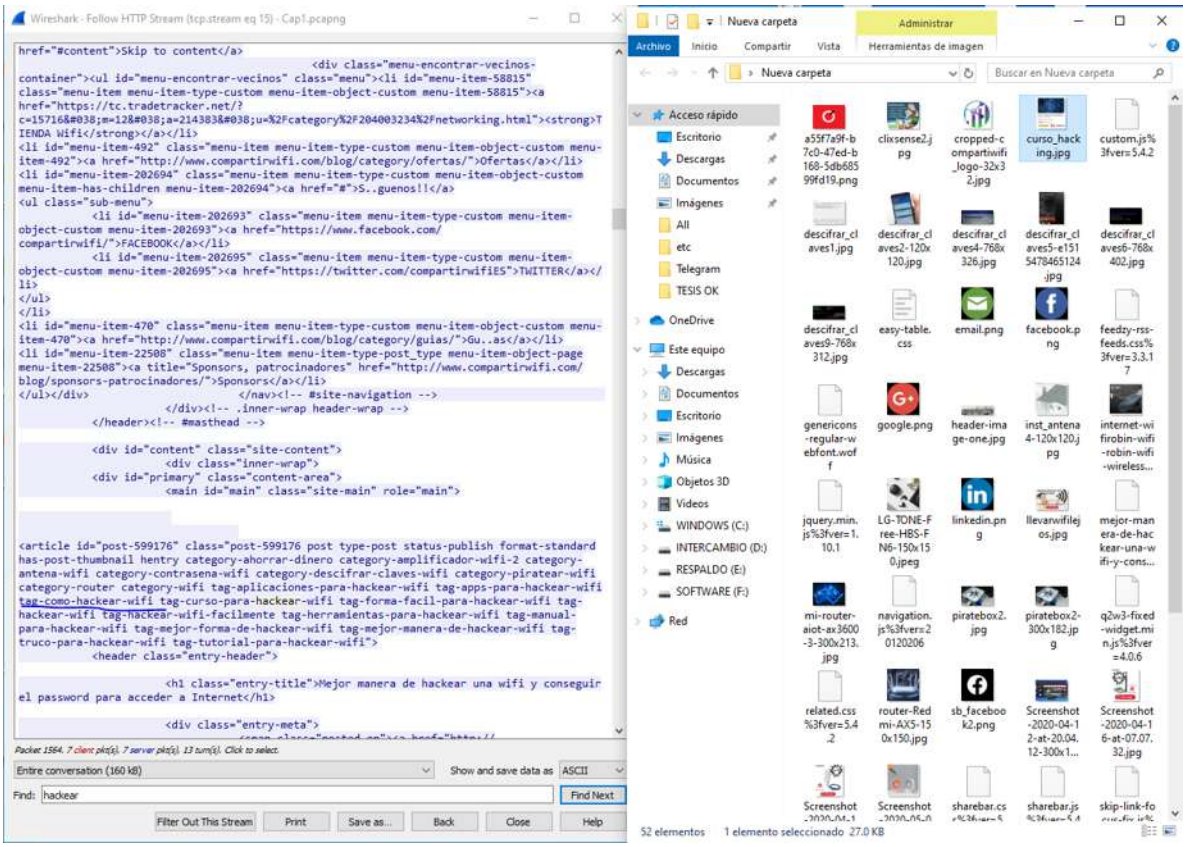



Figura 3.7. Resultados de la captura de trafico de red en el protocolo HTTP
*Fuente: Elaboración propia*

Así entonces, cuando se accede a un portal web, se puede hacer escribiendo en el buscador la URL de la página a consultar, o lo podemos hacer mediante un buscador, por ejemplo, Google. Pensando que la opción elegida fue escribir la URL en el buscador de *Internet,* al momento de dar *enter,* lo primero que hará nuestro equipo es, ir a solicitar la información al servidor de nuestro proveedor, a este servidor se le conoce como *resolutor,* el cual entenderá que el usuario le está preguntando si conoce la ubicación de la página consultada, si la respuesta es afirmativa, le indicará la dirección IP pública del equipo donde se encuentra almacenada la página web, para que el equipo del usuario pueda establecer una conexión con el servidor e intercambiar información de punto a punto sin pasar por otro servidor resolutor.

Esto se relaciona con el trabajo en cuestión debido a que todos los servicios de nube a los que se accede mediante *Internet,* responden a una consulta DNS para poder iniciar la conexión entre el usuario y el servidor donde reside el contenido. No obstante, es importante dejar en claro que en esta interacción no interviene voluntariamente el responsable del tratamiento de los datos personales, por ende, la responsabilidad del tratamiento de la información que se describe anteriormente, es responsabilidad de los servidores DNS y no de la empresa o persona con quien se lleva a cabo la interacción de manera consciente.

Por ello, es necesario establecer responsabilidades también para estas empresas, y no solo dejar la responsabilidad a las partes que se encuentran al final del árbol de interacción. Aunque de cierta manera, si hay una responsabilidad mayor en cuestión del tratamiento de datos personales por el responsable, no deja de ser importante mitigar el uso que se le da a la información del comportamiento de los usuarios en la red.

### *3.5. Instrumentos normativos nacionales e internacionales*

Como ya se ha mencionado anteriormente, la legislación en materia de protección de datos personales, en sus inicios, se planteó como un instrumento que limitara el uso de la informática para garantizar el respeto a la privacidad. Sin embargo, el hecho de limitar el uso de la tecnología para el procesamiento de la información,

podría llegar a repercutir en el sector económico, de tal manera que es necesario que la normativa tenga la flexibilidad para propiciar el libre flujo de información, sin perder de vista los derechos de los titulares de los datos que circulan por la red, mismos que se almacenan en bases de datos, sean locales o en la nube.

Para lograr este objetivo, se han realizado grandes esfuerzos que derivaron en la creación de diversos documentos de observancia nacional e internacional, en los cuales se han plasmado los principios rectores del tratamiento de los datos personales, mismos que, de cumplirse, se presupone la garantía del respeto a la privacidad de los titulares, sin violentar sus derechos ni restringir la circulación de los datos para efectos de comercio entre las naciones.

En tal sentido, si lo que se busca regular con dichas leyes es una tecnología universal, entonces las leyes deberían también ser internacionales o a menos, que los marcos normativos fuesen internacionales, mientras que las leyes estatales incorporen mecanismos de operación de la normativa internacional, solo así se podría hablar de una misma regulación, que regule el tratamiento de los datos personales en el entorno digital, por ser la misma tecnología a nivel mundial.

Al no existir una ley internacional, es necesario adherirse a los convenios existentes y/o tratados internacionales en materia de protección de datos personales, de esta manera, bajo los preceptos del artículo 133 constitucional, se hace obligatoria la observancia de lo que en dichos documentos se establezca, además como país miembro, lo dispuesto en tales convenios es vinculante y genera sanciones por el incumplimiento de lo dispuesto.

Dicho lo anterior, al ser integrante México de la Organización para la Cooperación y el Desarrollo Económico; del Foro de Cooperación Económica Asia-Pacífico; del Convenio 108 del Consejo de Europa y de la Organización de las Naciones Unidas, se hace obligatoria la adecuación de las leyes para el cumplimiento de lo establecido en la normativa emitida en materia de protección de datos personales, la cual, por su relevancia en el ámbito internacional, se retoman los siguientes documentos normativos nacionales e internacionales.

*A. Normativa de observancia internacional*

Por consiguiente, amanera de guía, se presenta un compilado de los documentos de observancia en materia de protección de datos personales en el ámbito internacional, comenzando por orden de antigüedad, se encuentran las *Directrices de la OCDE que Regulan la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales,* directrices en las que, desde 1980, se reconocen ocho principios fundamentales que han sido los pilares de protección en el tratamiento de los datos personales, a saber: Principio de limitación de recogida; principio de calidad de los datos; principio de especificación de los fines; principio de limitación de uso; principio de salvaguarda de la seguridad; principio de transparencia; principio de participación individual y principio de responsabilidad[186].

En el mismo sentido de ideas, se encuentra el *Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*[187] (Convenio 108) de 1981, dicho documento establece en sus principios, a) los compromisos de las partes; b) la calidad de los datos; c) las categorías particulares de datos; d) la seguridad de los datos; e; las garantías complementarias para la persona concernida; f) la excepción y restricciones; g) sanciones y recursos y h) protección más amplia.

De igual manera, la resolución 45/95 de la Asamblea General de la ONU de 1990, que se denominó, *Principios rectores sobre la reglamentación de los ficheros computarizados de datos personales*[188]*,* en dicho documento, la ONU, retoma los principios de los documentos anteriores con algunas adecuaciones terminológicas, quedando para este documento los principios rectores siguientes: Principio de la licitud y lealtad; principios de exactitud; principio de finalidad, principio de acceso de la persona interesada; principio de no discriminación y principio de seguridad.

---

[186] *Cfr.* OCDE, *Directrices de la OCDE que Regulan la Protección de la Privacidad…, Op. Cit.* p. 5.
[187] Cfr. Consejo de Europa, *Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal,* 1981, https://rm.coe.int/16806c1abd. Consultado: 17/05/2020.
[188] *Cfr.* Organización de las Naciones Unidas, Principios Rectores para la Reglamentación de los Ficheros Computadorizados de Datos Personales http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2015.pdf. Consultado: 23/05/2020.

Así mismo, la Comisión Europea en el año 1995, elaboró la *directiva 95/46/CE*[189]*,* en la cual se ampliaban los principios contenidos en otros instrumentos internacionales, e impedía que se crearan barreras que limitaran el libre flujo de los datos entre los estados miembros de la Comunidad Europea, esta directiva ha sido derogada por el *Reglamento General de Protección de Datos del Consejo de Europa* del que se ha hablado anteriormente.

En el mismo tenor, se localiza el *Marco de Privacidad del Foro de Cooperación Económica Asia–Pacífico*[190] *(APEC, por sus siglas en inglés),* conocido también como el Marco de Privacidad del APEC de 1999, el cual busca un equilibrio entre la seguridad de los datos personales y el libre flujo de la misma para propiciar el comercio, aprovechando las tecnologías de la información sin vulnerar los derechos humanos. Para ello, se establecen nueve principios, a saber: 1. Prevención del daño; 2. Aviso; 3. Limitación de recolección; 4. Uso de la información personal; 5. Elección; 6. Integridad de la información personal; 7. Medidas d seguridad; 8. Acceso y corrección y 9. Responsabilidad.

Por su parte, la Red Iberoamericana de Protección de Datos, en 2007 emitió las *Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana,* en dicho documento se reconoce el derecho a la protección de datos personales y deja claro que "[…] es preciso que los poderes públicos adopten las medidas necesarias para garantizar a las personas la salvaguarda del derecho fundamental, como garantía esencial del estado de derecho"[191], además señala que "[…] encontrándose plenamente garantizado el derecho fundamental, los Estados Iberoamericanos se beneficien del enriquecimiento económico, social y cultural que puede derivarse del libre intercambio transfronterizo de la información que contiene datos de carácter personal"[192].

---

[189] *Cfr.* 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 estos datos, https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=EN. Consultado: 17/05/2020.

[190] APEC, Marco de Privacidad http://www.apecsec.org.sg/apec/news__media/fact_sheets/about_apec.html. Consultado: 20/01/2020.

[191] Red Iberoamericana de Protección de Datos, Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana, 2007, p. 4, http://www.redipd.es/actividades/encuentros/V/common/9_nov/Directrices_de_armonizacion.pdf. Consultado: 21/01/2020.

[192] *Idem.*

Otro documento de importancia internacional, son los *Estándares Internacionales sobre protección de datos personales y privacidad. Resolución de Madrid,* se retoman la mayoría de los principios de los documentos anteriores, concentrando en este los principios de: lealtad y legalidad; finalidad; proporcionalidad; calidad; transparencia y responsabilidad. La finalidad de esta resolución es "definir un conjunto de principios y derechos que garantice la efectiva y uniforme protección de la privacidad a nivel internacional, en relación con el tratamiento de datos de carácter personal y facilitar los flujos internacionales de datos de carácter personal, necesarios en un mundo globalizado"[193].

Resalta de este documento lo que establece en cuanto a las medidas proactivas, que establecen la necesidad de realizar revisiones continuas para la detección y prevención de infracciones; la designación de un oficial de seguridad de datos personales; la realización de programas de concienciación, educación y formación; realizar auditorías de cumplimiento de la legislación aplicable; adoptar sistemas tecnológicos destinados al tratamiento de datos personales; realizar estudios de impacto sobre privacidad previo a la implementación de nuevos sistemas tecnológicos; recomienda la adhesión a acuerdos de autorregulación, así como la implementación de planes de contingencia[194].

Por último, el documento más importante en el ámbito internacional, es el *Reglamento General de Protección de Datos del Consejo de Europa*, del cual ya se realizó un análisis en este capítulo, cabe precisar que derivado de la adhesión de México al Convenio 108, resulta de aplicabilidad en el tratamiento de los datos personales para las empresas mexicanas.

No obstante, entre más normativa se tiene que observar, las complicaciones de cumplimiento aumentan. Por tal motivo, es recomendable hacer un documento propio en el que, de acuerdo a los tipos de datos personales, el entorno en el que se traten y los medios de recolección, se adecue al cumplimiento de manera particular, es decir, si no se tratan datos sensibles, no hay necesidad de informar

[193] *Cfr.* Agencia Española de Protección de Datos, Estándares Internacionales sobre Protección de Datos Personales y Privacidad. Resolución de Madrid, 2009, pp. 9–13, https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf. Consultado: 21/01/2020.
[194] *Ibidem,* pp. 24–25.

sobre tales tratamientos, ni de implementar mecanismos tecnológicos para la recogida del consentimiento tácito del titular, pero si es necesario que el aviso de privacidad contemple de manera amplia los principios, y explique al titular de manera sencilla y clara, todo lo necesario para que pueda ejercer su derecho a la autodeterminación informativa con respecto a sus datos.

En el territorio nacional, también se han realizado grandes esfuerzos para armonizar la legislación local con la normativa internacional, con la intención de poder establecer relaciones comerciales, sin perjuicios de violaciones al derecho a la protección de los datos personales de los residentes de países en los que la legislación, prohíbe estrictamente transferir información de sus ciudadanos, a estados en los que no se cuenta con una legislación en materia de protección de datos personales, acorde a los principios rectores del tratamiento de datos personales del país de origen. Ejemplo de ello, es la legislación europea, que ha sido determinante para la legislación mexicana que se presenta a continuación.

*B. Normativa de observancia nacional*

En México, como se ha establecido en el artículo 133, la Constitución y todas las leyes del congreso aprobadas por el senado, así como los tratados celebrados y que se celebren por el presidente, serán la Ley Suprema. Por lo que el tratamiento de datos personales deberá, en primer lugar, garantizar los derechos consagrados en la Constitución, en tal sentido, la Ley en materia de protección de datos personales, es una ley reglamentaria del artículo 6° constitucional, apartado B, 16° y 73°, dando como resultado la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de la cual se ha hablado anteriormente.*

Así entonces, hablando específicamente del tratamiento de datos personales en posesión de los particulares, solo existe una Ley de observancia, dicha ley cuenta con su reglamento, *–Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares–.* Por otro lado, a manera de orientación para la elaboración de los avisos de privacidad, la Secretaría de Economía, por atribuciones establecidas en la Ley, emitió los *Lineamientos del Aviso de*

*Privacidad*[195]*,* en el cual se incluyen los elementos que debe contener el aviso de privacidad y los tipos de avisos de privacidad de los que se habla en el segundo capítulo.

Además de los documentos anteriores, se deben tener en cuenta los *Parámetros de Autorregulación en Materia de Protección de Datos Personales*[196]*,* emitidos por la Secretaría de Economía, de los cuales derivó la *Guía de Esquemas de Autorregulación en Materia de Protección de Datos Personales*[197], emitidos por el INAI. Cabe señalar que, en México, a diferencia de otros países, la autorregulación si tiene efecto vinculante, es decir que las infracciones a dichos esquemas de autorregulación, pueden derivar en sanciones según las establecidas en el esquema de autorregulación. Cabe señalar que los esquemas de autorregulación, pueden ser de tres tipos:

> I. Las reglas emitidas con objeto de adaptar la normativa aplicable en materia de protección de datos personales a la realidad y actividades de un sector en particular, a fin de hacer eficiente la aplicación del derecho a su protección;
> II. Los esquemas de autorregulación vinculante evaluados y validados por el Instituto cuando satisfagan todos los requisitos previstos para ello, denominados esquemas con validación, que tendrán por objeto elevar los estándares de protección de datos personales y adoptar las mejores prácticas en la materia, y
> III. Los esquemas de autorregulación vinculante certificados por un organismo de certificación en materia de protección de datos personales, que serán reconocidos por el Instituto a través de su inscripción en el Registro, denominados esquemas con certificación reconocida, que también tendrán por objeto elevar los estándares de protección de datos personales y adoptar las mejores prácticas en la materia[198].

Además de tener como finalidad la implementación de buenas prácticas en el tratamiento de datos personales, los esquemas de autorregulación pueden ser tomados en cuenta para atenuar las sanciones de posibles infracciones a la Ley. No

---

[195] Diario Oficial de la Federación, Lineamientos del Aviso de Privacidad, Secretaría de Economía, 2013, http://www.dof.gob.mx/nota_detalle.php?codigo=5284966&fecha=17/01/2013. Consultado: 17/01/2020.
[196] Diario Oficial de la Federación, Parámetros de Autorregulación en Materia de Protección de Datos Personales, Secretaría de Economía, 2014, https://www.economia.gob.mx/files/marco_normativo/PAR1.pdf. Consultado: 17/01/2020.
[197] INAI, Guía de Esquemas de Autorregulación en Materia de Protección de Datos Personales, 2016, http://cevifaiprivada.ifai.org.mx/pluginfile.php/14423/mod_data/content/15/Gu%C3%ADa%20de%20Esquemas%20de%20Autorregulaci%C3%B3n%20en%20Materia%20de%20Protecci%C3%B3n%20de%20Datos%20Personales.pdf. Consultado: 18/01/2020.
[198] Diario Oficial de la Federación, Parámetros de Autorregulación…, *Op. Cit.* p. 6–6.

menos importante, también pueden servir para conservar o incrementar la reputación de la empresa al generar la expectativa de responsabilidad y garantías de los derechos de los titulares.

El INAI, en aras de cumplir con las obligaciones en materia de difusión del derecho a la protección de datos personales, ha emitido guías para los usuarios, mismas que deben ser tomadas en consideración por los responsables para conocer los derechos que los titulares tienen y que pueden ejercer ante ellos. Tal es el caso de la *Guía para el Tratamiento de Datos Biométricos*[199]*;* Guía para Titulares de los Datos Personales Volumen 1, 2, 3 y 4. Denominadas: Conceptos Generales de la Protección de Datos Personales[200]; Principios Rectores de la Protección de Datos Personales[201]; Los derechos ARCO[202] y Procedimientos de datos personales ante el INAI[203], respectivamente.

En caso de que, al momento de hacer la recolección de los datos personales, el responsable no haya exhibido el aviso de privacidad, puede recurrir a lo establecido en la *Guía para instrumentar medidas compensatorias*[204]*,* emitida por el INAI en 2016. En un principio se pensó en esta guía para que todas las empresas que habían recolectado datos personales previo al a entrada en vigor de la Ley, instrumentaran medidas para hacer del conocimiento de los titulares, las condiciones a las que estaban sometidos sus datos personales. No obstante, si se da el caso, las empresas aún pueden recurrir a tal guía para dar a conocer el aviso de privacidad, en caso de no haber cumplido en tiempo y forma con la puesta a disposición del mismo al titular de los datos.

---

[199] INAI, Guía para el Tratamiento de Datos Biométricos, 2018, http://inicio.ifai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf. Consultado: 11/01/2020.
[200] INAI, Conceptos General de la Protección de Datos Personales, 2019, https://www.cinvestav.mx/Portals/0/sitedocs/tyr/GuiaTitulares-01_PDF.pdf. Consultado: 12/01/2020.
[201] INAI, Principios Rectores de la Protección de Datos Personales, 2019, https://www.cinvestav.mx/Portals/0/sitedocs/tyr/GuiaTitulares-02_PDF.pdf. Consultado: 11/01/2020.
[202] INAI, Los Derechos ARCO, 2019, https://www.cinvestav.mx/ Portals/0/sitedocs/tyr/GuiaTitulares-03_PDF.pdf. Consultado: 11/01/2020.
[203] INAI, Procedimientos de datos personales ante el INAI, 2019, https://www.cinvestav.mx/Portals/0/sitedocs/tyr/GuiaTitulares-04_PDF.pdf. Consultado: 11/01/2020.
[204] INAI, Guía para instrumentar medidas compensatorias, 2016, http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_para_instrumentar_medidas_compensatorias.pdf. Consultado: 12/01/2020.

En cuanto a los mecanismos de defensa contra las resoluciones del órgano garante, se deben observar el *Código Federal de Procedimientos Civiles* y de la *Ley Federal de Procedimiento Administrativo.* Así, en caso de no estar conformes con las resoluciones del INAI se puede proceder con el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.

Así entonces, a continuación, se enlistan los documentos legales y guías emitidas para el cumplimiento de la Ley, y para conocimiento de los titulares del derecho a la protección de datos personales:

1. Constitución Política de los Estados Unidos Mexicanos.
2. Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
3. Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
4. Código de Comercio
5. Ley Federal de Protección al Consumidor
6. Lineamientos de Avisos de Privacidad
7. Parámetros de Autorregulación en Materia de Protección de Datos Personales.
8. Código Federal de Procedimientos Civiles
9. Ley Federal de Procedimiento Administrativo.
10. Guía de Esquemas de Autorregulación en Materia de Protección de Datos Personales.
11. Guía para el tratamiento de datos biométricos
12. Guía para titulares de los datos personales Volumen 1. Conceptos Generales de la Protección de Datos Personales.
13. Guía para titulares de los datos personales Volumen 2. Principios rectores de la protección de datos personales.
14. Guía para titulares de los datos personales Volumen 3. Los derechos ARCO
15. Guía para titulares de los datos personales Volumen 4. Procedimientos de datos personales ante el INAI.

Como se ha notado, son varios los documentos que se deben observar en torno al tratamiento de los datos personales, esto no significa que todos ellos sean distintos, en su mayoría versan sobre los principios, deberes y obligaciones de los responsables, así como de los derechos de los titulares, los mecanismos y guías de orientación para ejercer sus derechos ante los titulares y ante el órgano garante.

Es por ello que se considera importante el conocimiento de todos y cada uno de ellos para cumplir con el deber informativo de manera adecuada, y brindar proactivamente, orientación a los titulares para el ejercicio de sus derechos.

### *3.6. Reflexiones finales*

Resulta interesante analizar cómo las empresas que realizan comercio electrónico, pueden tener cierta ventaja contra aquellas que siguen utilizando los canales tradicionales para la compraventa de productos y servicios. Sin embargo, cada vez son más las empresas que se suman al entorno digital, ofertan sus productos y servicios de manera más eficiente y a costos menos elevados gracias a las herramientas del comercio electrónico.

No obstante, el uso de las tecnologías de comercio electrónico requiere de información para poder concretar las transacciones entre el comprador –titular de los datos– y el vendedor –responsable de su tratamiento–, dicha información, no solo es recolectada por la empresa que realiza la venta del producto o servicio, sino que, también intervienen terceras empresas como intermediarias de las transacciones de dinero, empresas de paquetería para la entrega de los productos y empresas tecnológicas, que sin darnos cuenta, están recolectando la misma cantidad o incluso más información de la que se entrega a quien se presenta como el responsable del tratamiento de los datos que, voluntariamente y de manera informada –en ocasiones–, se entrega a las empresas.

De tal manera que cuando se realizan compras en alguna de las plataformas de comercio electrónico, fácilmente se puede encontrar el aviso de privacidad, en donde se informa, de acuerdo a lo que establece la Ley, todo lo necesario respecto al tratamiento que se hará de los datos personales, para así, estar en condiciones de ejercer el derecho a la autodeterminación informativa.

Esto parece ser un acto que cumple con los principios, deberes y obligaciones que rigen el tratamiento de los datos personales, de no ser porque detrás de dichas transacciones existen otras tecnologías de recolección silenciosa, que pueden almacenar un elevado número de datos de identificación personal. Cuando estas son utilizadas de manera intencional por la empresa con la que se está celebrando la transacción comercial, deberá informar detalladamente sobre ello, además de tener en cuenta el principio de proporcionalidad.

Lo más común en relación a lo anterior, es que las empresas con las que se realiza la transacción, no sean las responsables directas de la recolección silenciosa de los datos, sino, solo las detonantes de dicha actividad por empresas como Google, Apple o Facebook, las cuales tienen un especial interés por analizar lo que las personas hacen en la red, para mejorar el servicio de publicidad que venden a otras empresas comerciales.

Con dicha información se genera un perfil digital de cada persona, brindando a la empresa poseedora de esa información, una ventaja competitiva en el mercado de los servicios de publicidad focalizada, esto se puede realizar mediante tecnologías de *Big Data,* inteligencia artificial, minería de datos, entre otras, que pueden derivar en violaciones a la privacidad e incluso recolectar datos sensibles, que, de acuerdo a la Ley, requieren del consentimiento tácito para su tratamiento y que, gracias a estas tecnologías, pueden ser recolectados y usados con fines mercadotécnicos, sin el consentimiento de los titulares de dichos datos.

Así entonces, cuando se usan los servicios tecnológicos que parecen ser gratuitos, en realidad se están cobrando con los datos que recolectan, estas son cuestiones que las mismas MIPYMES que realizan comercio electrónico desconocen, por ello, parece coherente que los avisos de privacidad no informen de manera adecuada sobre las tecnologías utilizadas para la recolección de datos, o sobre las trasferencias de los mismos a terceras empresas, que no encajan en las excepciones de la Ley, como ya se mencionaba con anterioridad, podrían ser las empresas que realizan las transacciones de dinero.

En consecuencia, el desconocimiento es un factor importante que no se cubre con la legislación, por su parte la legislación mexicana denota algunas debilidades

en cuanto a la organización de la información, la claridad y la especificidad de la misma; en relación al *Reglamento General de Protección de Datos del Consejo Europeo,* en el cual se observa una estructura más ordenada, y más explicada para que los sujetos regulados, puedan adoptar las medidas y técnicas necesarias para el cumplimiento de la Ley. Por ello, se considera que, en México, aún se deben mejorar algunos aspectos de la Ley.

Lo anterior no significa que la legislación mexicana sea deficiente, no olvidemos que México se adhirió en el año 2018 al *Convenio 108,* lo que demuestra que la legislación, en contenido, cumple con los requisitos mínimos necesarios que se exigen en la legislación europea, como se recalca, parece ser más un problema de desconocimiento que de regulación.

Otro aspecto importante a tener en cuenta, es el órgano garante de dicho derecho humano, ya que como se observa en la resolución PPD.02.13/16[205], el mismo órgano garante de este derecho, desconoce el funcionamiento de la tecnología, motivo por el cual, no se puede esperar una adecuada protección del derecho a la protección de datos personales.

Lo anterior, ha propiciado que las empresas sigan haciendo uso de los datos de manera irregular, violando principios como la proporcionalidad, el consentimiento e incluso algunas de ellas ni siquiera tengan un aviso de privacidad, en el que informen sobre el tratamiento de los datos personales, tal como se puede observar en la tabla 3.1 que se muestra en este capítulo.

[205] *Cfr.* INAI, *Expediente PPD.02.13/16,* 2016, http://inicio.ifai.org.mx/pdf/resoluciones/2016/PPD%200213.pdf. Consultado: 20/06/2020.

*Todo es práctica*

*- Pelé -*

# CAPÍTULO CUARTO

## PROPUESTA JURÍDICO–TÉCNICA PARA LA ARMONIZACIÓN ENTRE TECNOLOGÍA Y EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

### *4.1. Los retos de la autodeterminación informativa en el proceso de recolección de datos personales en sistemas de cómputo en la nube*

En la actualidad la información es poder, por tal motivo las empresas tecnológicas dedicadas a la venta de servicios publicitarios, recolectan cada vez más información para su procesamiento y creación de perfiles de usuario. Incluso, empresas del sector comercial y/o de servicios, pueden hacer uso de las tecnologías de *BigData* para la recolección de información de redes sociales, para obtener conocimiento respecto a patrones de consumo de los clientes, y con ello, orientar sus campañas publicitarias, esto genera poder competitivo y adquisitivo en el mercado.

Por su parte los ciudadanos, titulares de los datos que tratan estas empresas, requieren de información por parte del responsable para poder ejercer los derechos ARCO, de esta manera, el titular podrá ejercer su autodeterminación informativa con base en la información que se le proporcione, asimismo, para el ejercicio de sus derechos, es necesario que el responsable establezca algún procedimiento para facilitar su ejercicio.

Para tal efecto, las empresas están sujetas a la legislación en materia de protección de datos personales, por ello, al hacer uso de plataformas de comercio electrónico, deben mostrar en su portal web el aviso de privacidad, el cual, por lo regular se coloca en la parte inferior, en ocasiones, dependiendo del diseño, puede colocarse en la parte superior o del lado izquierdo, dependiendo de donde sea más visible para el cliente.

Sin embargo, se debe considerar que no existe una cultura de información, y por lo regular estos avisos de privacidad pasan por desapercibidos. No obstante, los clientes que tácitamente aceptan las condiciones de este aviso de privacidad, estarán celebrando un contrato de adhesión con el responsable, quien deberá velar por la seguridad y confidencialidad de los datos.

Por tanto, cuando se recolectan datos personales, el aviso de privacidad hace la función de un contrato de adhesión mediante el cual, el responsable se obliga a proteger los datos conforme a la Ley, y el titular de los datos se adhiere a dicho tratamiento, entendiendo que, al no manifestar oposición a lo establecido en dicho aviso, se presupone que consciente que el responsable trate sus datos bajo las condiciones redactadas unilateralmente por el responsable del tratamiento.

En consecuencia, el responsable debe contar con elementos para probar que el titular consciente el tratamiento de sus datos, para ello, se debe considerar el consentimiento expreso, el cual se prueba mediante una casilla de verificación que no debe estar seleccionada por default, dejando la libertad al titular de elegir si acepta o no los términos informados.

Cabe señalar que cuando se trata de datos personales sensibles, el responsable no podrá hacer uso de este método para recolectar el consentimiento, pues para este caso se requiere el consentimiento tácito y por escrito, lo cual supone que, para ciertos servicios, las empresas deberán implementar mecanismos de firma electrónica, campos de captura mediante tabletas o cuadros de captura de dibujo para firma. De otra manera, no sería posible contar con el consentimiento de los titulares para poder tratar dichos datos.

En relación a lo anterior, resulta de interés lo que la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* enuncia en el artículo 10, ya que en este se encuentra el fundamento legal para poder realizar el tratamiento de los datos, claro está con la excepción de los datos personales sensibles:

> Artículo 10.- No será necesario el consentimiento para el tratamiento de los datos personales cuando:
> I. Esté previsto en una Ley;
> II. Los datos figuren en fuentes de acceso público;
> III. Los datos personales se sometan a un procedimiento previo de disociación;
> IV. Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;
> V. Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
> VI. Sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones jurídicas

aplicables y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente, o

VII. Se dicte resolución de autoridad competente[206].

Dicho lo anterior, el reto más grande respecto a la autodeterminación informativa ante el uso de la tecnología, es la comprensión de la Ley para, en base a ello, estructurar toda la información necesaria que el titular debe conocer con respecto al tratamiento de los datos personales que de él se recolectan, la finalidad para la cual se recolectan, el periodo de conservación, si se comparte con otras empresas o fuera del territorio nacional y con qué fines, los derechos que tiene la persona –Derechos ARCO–, los procedimientos para ejercer cada uno de esos derechos, el contacto para el ejercicio de sus derechos, que tecnologías de recogida de datos se utilizan; si se utilizan tecnologías de monitoreo y/o seguimiento del comportamiento del usuario en *Internet;* si se han adoptado medidas de seguridad de los datos, que medidas se han adoptado para la protección de menores, así como implementar mecanismos que faciliten el ejercicio de los derechos y, hacerlos saber en el mismo aviso de privacidad.

Con todos estos elementos, los titulares de los datos podrán estar en condiciones de decidir libremente si desean que sus datos sean tratados bajo esas condiciones. En el tema de inclusión y a manera de ser proactivos, se pueden generar los avisos de privacidad en audio y en los idiomas o dialectos en los que se comercialicen los productos y servicios de la empresa.

Si se cubren estos elementos, se estará cumpliendo con el principio de información. En consecuencia, solo se debe cuidar que el tratamiento que se dé a la información, cumpla con el resto de los principios para que no se considere ilegal, ello garantiza que las empresas respeten el derecho a la autodeterminación informativa, la cual también se relaciona con el libre desarrollo de la personalidad, de manera informada.

Por consiguiente, para la recolección del consentimiento del titular de los datos, es necesario que, en los formularios de recolección de datos, siempre exista la casilla de verificación para que el usuario manifieste la aceptación de los términos

[206] *Ley Federal de Protección de Datos Personales…, Op. Cit.* Artículo. 37, p. 9

del aviso de privacidad, este elemento no debe esta seleccionado por default, sino, debe ser seleccionado a voluntad del titular de los datos, de esta manera se cumple con la libertad de autodeterminación informativa del usuario.

*4.2. Normatividad aplicable*

La normativa aplicable resulta extensa cuando se trata de garantizar la seguridad de los datos, pues para poder cumplir con la Ley, es necesario también aplicar metodologías internacionales, códigos de buenas prácticas y observar la normativa que, de alguna manera interviene en el proceso del tratamiento de los datos personales, sea para reconocer los actos jurídicos entre el responsable y el titular o para garantizar la protección del titular como cliente.

En tal sentido, se puede observar que existe una regulación propia del tratamiento de datos personales, misma que es de obligada observancia, además, existen otras leyes que pueden aplicar dependiendo del giro de la empresa o que sirve como apoyo para la solución de controversias en los procedimientos de protección de derechos ante el NAI o ante el Tribunal Federal de Justicia Administrativa, tales regulaciones son las siguientes.

Regulación del tratamiento de datos personales: Artículos 1, 16 y 73 de la *Constitución Política de los Estados Unidos Mexicanos; Ley Federal de Protección de Datos Personales en Posesión de los Particulares; Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; Lineamientos del Aviso de Privacidad* y su anexo referente a las *Buenas Prácticas en el Aviso de Privacidad; Parámetros de Autorregulación en Materia de Protección de Datos Personales; Recomendaciones en materia de Seguridad de Datos Personales, y el Acuerdo por el que se establece el sistema electrónico para la presentación de solicitudes de protección de derechos y de denuncias, así como la sustanciación de los procedimientos previstos en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Documentos a los que se puede encontrar la referencia en la bibliografía de este documento.*

En lo que respecta a la regulación para la conservación, se enlistan las siguientes Leyes y códigos de obligada observancia: *Código de Comercio; Código Fiscal de la*

*Federación; Reglamento del Código Fiscal de la Federación; Ley Federal de Protección al Consumidor.*

A continuación, se presenta la propuesta para el análisis de riesgos, los datos a los que se hace referencia son ficticios y solo a manera de ejemplo, por lo que no se deben tomar como parámetros reales al momento de elaborar el propio análisis de riesgos.

### *4.3. Principales elementos del documento de seguridad como guía para la implementación de medidas de seguridad*

Si bien el documento de seguridad debe abarcar más temas de los que se plantean en este apartado, aquí se brinda una guía orientada a cumplir con las medidas de seguridad y los principios rectores del tratamiento de los datos personales, sin embargo, para lograr cubrir en su totalidad los requerimientos para este documento, es recomendable tomar como referencia las normas ISO 31000; ISO 27005; ISO 27001; ISO 27002; ISO 27018; ISO 27701; NIST SP800-30; Octave Allegro, ITIL, Magerit, por mencionar las más importantes.

Es necesario precisar, que las medidas de seguridad de la información, son esenciales para la protección de los datos personales, así como para el cumplimiento de lo establecido en el artículo 19 de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares.* En tal sentido, cuando se trata de sistemas de cómputo en la nube, se tiene la expectativa de que el proveedor ha implementado la seguridad pertinente, para garantizar que los datos contenidos en sus servidores permanecerán seguros, íntegros y confidenciales ante terceros no autorizados.

No obstante, los dispositivos desde los cuales se accede a los sistemas de cómputo en la nube, también suponen un vector de ataque para los delincuentes informáticos, que puede poner en riesgo la integridad y confidencialidad de información. Por ello, es necesario implementar mecanismos de seguridad administrativa, técnica y física al interior de la empresa, ya que, aunque los datos se almacenan en la nube, los equipos mediante los cuales se accede a los sistemas pueden ser vulnerados.

Con la intención de aclarar el punto anterior, es preciso retomar el diagrama de la figura 4.1, donde se enuncian los actores que propone el Instituto Nacional de Estándares y Tecnología *(National Institute of Standards and Techonology, NIST),* donde se muestran los posibles intervinientes en el tratamiento de los datos personales en el proceso de llevarlos hasta el destino final, donde permanecerán almacenados y serán tratados por el responsable.

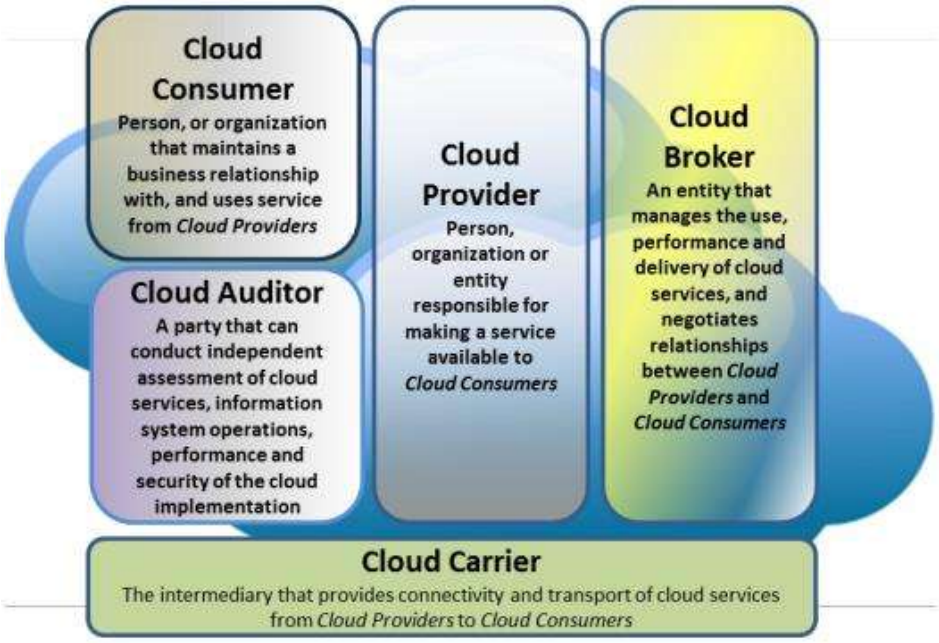



Figura 4.1. Actores del cómputo en la nube.
*Fuente: NIST Cloud Computing Standards Roadmap, 2013, p. 12.*

De acuerdo a este supuesto, el responsable del tratamiento de los datos personales ante la Ley, pierde el control de la información mientras pasa por los servidores de los intervinientes, de tal suerte que no le será posible cumplir con los requisitos establecidos en la Ley y su reglamento, en concreto, con el artículo 52 del reglamento, en el que se enlistan los requisitos y supuestos en los que el responsable podrá hacer uso del cómputo en la nube.

Requisitos que resulta complejo cumplir al pie de la letra, por lo que la alternativa a este problema es realizar los esfuerzos que estén al alcance del responsable, para que los datos que se envíen a los sistemas de cómputo en la nube, no sean alterados, interceptados o accedidos en las infraestructuras del responsable. Para

ello, se deben implementar medidas de seguridad, así como mecanismos de encriptado.

Entre otras acciones, es necesario hacer campañas de concientización de los usuarios en relación a los riesgos derivados del uso de los equipos de cómputo, manejo de contraseñas, instalación de software, uso del correo electrónico; medio por el cual se propaga malware, sitios de engaño *(phishing)* o ransomware, uno de los virus más temidos en la actualidad, también conocido como virus de secuestro de información. La forma en la que operan es mediante la encriptación de la información y, una vez que la información está encriptada, se solicita el rescate de la misma, aunque el pago de dicho rescate no garantiza la recuperación de la información.

El medio más utilizado para la propagación de este virus, es el correo electrónico y los archivos PDF, por tanto, es necesario que los usuarios aprendan a revisar el contenido, así como la procedencia de los correos para no caer en engaños que deriven en la vulneración de la seguridad, ya que algunas variantes de este virus tienen la capacidad para detectar conexiones a plataformas de nube, y encriptar todo lo que se encuentre almacenado en ellas.

De igual manera, es importante mantener los antivirus actualizados, aunque no existe ningún antivirus que garantice la seguridad total contra virus que tengan como finalidad extraer información o acceder a los datos de las empresas, sí son una herramienta de protección que ayuda a disminuir el riesgo de que esto suceda. Los mejores antivirus del mercado en la actualidad son: *BullGuard, McAfee, Bitdefender, Norton, Panda y Kaspersky*[207], aunque como ya se dijo anteriormente, no garantizan la seguridad de la información, por ello la necesidad de capacitar y concientizar a los usuarios de las tecnologías.

Para dar cumplimiento a las medidas de seguridad requeridas, a continuación, se presenta la propuesta de las acciones a tener en cuenta, comenzando con la elaboración del documento de seguridad, el cual tiene como finalidad presentar un panorama general de la organización, y a partir de ello determinar las medidas de

[207] TopReviews, *Comparativa antivirus 2020.* 2020, https://www.topreviews.eu/es/mejor-antivirus/ Consultado: 10/07/2020.

seguridad pertinentes para garantizar la confidencialidad de la información y el respeto a los derechos de los titulares.

### *4.3.1. Guía para el cumplimiento de los principios rectores del tratamiento de datos personales*

Como requisito integrante del documento de seguridad y derivado del análisis de los avisos de privacidad de las empresas, en los cuales se observa un cierto desapego a los principios de la Ley, sobre todo en lo que respecta a la información sobre los datos personales que recolectan, a las finalidades primarias y secundarias, así como el procedimiento para el ejercicio de los derechos ARCO y la elaboración de documentos guía para facilitar el ejercicio de los mismos al titular, se presenta una propuesta de aviso de privacidad, el cual se puede tomar como base para la elaboración de uno propio, según los requerimientos del responsable.

Cabe señalar que este aviso de privacidad ha sido elaborado tomando como referencia los *Lineamientos del aviso de privacidad*[208]*,* documento elaborado por la Secretaría de Economía, por lo que se presupone que, al cumplir con lo establecido en dichos lineamientos, se estaría cumpliendo en su totalidad con los requisitos establecidos para este documento, el cual tiene la finalidad, cumplir con el principio de información y garantizar el respeto a la autodeterminación informativa del titular.

Cabe recordar que como se mencionó anteriormente, existen tres modalidades del aviso de privacidad. No obstante, en este apartado solo se presenta el aviso de privacidad integral, documento en el que se incluye la totalidad de los elementos requeridos por la Ley, mediante los cuales se le informa al titular sobre el tratamiento de sus datos personales y las condiciones de dicho tratamiento. A manera de propuesta se presenta el siguiente modelo de aviso de privacidad.

AVISO DE PRIVACIDAD INTEGRAL

“Razón Social de la empresa”, mejor conocido como “Nombre comercial de la empresa, con domicilio en calle “especificar calle”, colonia “especificar colonia”,

[208] *Cfr.* Diario Oficial de la Federación, *Lineamientos del Aviso de Privacidad… Op. Cit.*

ciudad “Escribir la ciudad”, municipio o delegación “municipio o delegación”, C.P. “escribir código postal”, estado de “escribir el nombre de la entidad federativa”, país “Escribir el país”, y portal de *Internet* “escribir la URL del portal de *Internet*, si existe”, es el responsable del uso y protección de sus datos personales, y al respecto le informamos lo siguiente:

¿Para qué fines utilizaremos sus datos personales?
Los datos personales que recabamos de usted, los utilizaremos para las siguientes finalidades que son necesarias para el servicio que solicita:

- Facturación (ejemplo)
- Responder a solicitudes de contacto (ejemplo)

*NOTA PARA EL LECTOR: agregar en este apartado las finalidades que son necesarias para el cumplimiento de la relación jurídica, mismas que de no ser aceptadas se presupone la cancelación del contrato de prestación del servicio.*

De manera adicional, utilizaremos su información personal para las siguientes finalidades secundarias que *no son necesarias* para el servicio solicitado, pero que nos permiten y facilitan brindarle una mejor atención:

- Estadísticas
- Mercadotecnia o publicitaria
- Prospección comercial

*NOTA PARA EL LECTOR: agregar en este apartado todas finalidades secundarias para las cuales utilizarán los datos personales del titular, se debe tener en cuenta que las finalidades no pueden ser contrarias a la finalidad primaria ni desproporcionadas, lo más común, son las finalidades publicitarias y de comunicación directa con el titular de los datos.*

En caso de que no desee que sus datos personales se utilicen para estos fines secundarios, deberá imprimir este aviso de privacidad y marcar con una X la casilla correspondiente del siguiente apartado, posteriormente deberá enviarlo escaneado al correo ejemplo@dominio.com.

No consiento que mis datos personales se utilicen para los siguientes fines:
[ ] Estadísticas
[ ] Mercadotecnia o publicitaria
[ ] Prospección comercial

La negativa para el uso de sus datos personales para estas finalidades no podrá ser un motivo para que le neguemos los servicios y productos que solicita o contrata con nosotros.

¿Qué datos personales utilizaremos para estos fines?

Para llevar a cabo las finalidades descritas en el presente aviso de privacidad, utilizaremos los siguientes datos personales:

- Nombre
- Registro Federal de Contribuyentes (RFC)
- Domicilio
- Teléfono particular
- Correo electrónico
- Puesto o cargo que desempeña
- Domicilio de trabajo
- Correo electrónico institucional
- Teléfono institucional
- Datos de identificación
- Datos de contacto

*NOTA PARA EL LECTOR: Enlistar aquí todos los datos necesarios para el cumplimiento de la finalidad primaria, tomando como principio la limitación de recogida, que se refiere a que los datos recolectados deben ser los mínimos necesarios para el cumplimiento de la relación jurídica contraída con el titular de los datos.*

¿Con quién compartimos su información personal y para qué fines?
Le informamos que sus datos personales son compartidos dentro del país con las siguientes personas, empresas, organizaciones o autoridades distintas a nosotros, para los siguientes fines:

| **Destinatario de los datos personales** | **Finalidad** | **Requiere del consentimiento** |
|---|---|---|
| Razón social de la empresa 1 | Ejemplo: Facturación | Sí |
| Razón social de la empresa 2 | Ejemplo: Compra en línea | Si |

*NOTA PARA EL LECTOR: Cuando se usa la información para facturación mediante el servicio de un tercero, el cual proporciona el almacenamiento del catálogo de clientes, se entiende que la información se transfiere a dicha empresa, por lo tanto, la información se comparte con la finalidad de emitir las facturas, aunque la empresa receptora de los datos no trate los datos, el titular debe conocer sobre este hecho debido a que su información queda en manos de un tercero.*

¿Cómo puede acceder, rectificar o cancelar sus datos personales u oponerse a su uso?
Usted tiene derecho a conocer qué datos personales tenemos de usted, para qué los utilizamos y las condiciones del uso que les damos (Acceso). Asimismo, es su derecho solicitar la corrección de su información personal en caso de que esté desactualizada, sea inexacta o incompleta (Rectificación); que la eliminemos de nuestros registros o bases de datos cuando considere que la misma no está siendo utilizada adecuadamente (Cancelación); así como oponerse al uso de sus datos personales para fines específicos (Oposición). Estos derechos se conocen como derechos ARCO.

Para el ejercicio de cualquiera de los derechos ARCO, usted podrá llenar el formulario de solicitud de derechos ARCO (AGREGAR HIPERVÍNCULO PARA SU DESCARGA) o presentar escrito de forma libre, a través del siguiente correo electrónico ejemplo@dominio.com, entregar escrito de manera personal o formular su solicitud de manera verbal en el domicilio del responsable, establecido en, *“especificar el domicilio y departamento responsable del trámite”.*

Con relación al procedimiento y requisitos para el ejercicio de sus derechos ARCO, le informamos lo siguiente:

a) ¿A través de qué medios puede acreditar su identidad el titular y, en su caso, su representante, así como la personalidad de este último?: Vía correo electrónico, mediante escrito o de manera verbal en el domicilio señalado anteriormente.

b) ¿Qué información y/o documentación deberá contener la solicitud? Nombre, Acta de nacimiento, INE o Credencial de elector, Pasaporte, Licencia de manejo, Cedula profesional, Documento migratorio FM2 o FM3. En caso de ser un representante legal, deberá anexar poder notariado o en su caso poder simple firmado ante dos testigos para acreditar su personalidad. En esta misma solicitud deberá mencionar algunos de los medios por los cuales desea que se le dé respuesta (correo electrónico, dirección postal "puede representar costo de reproducción y envío", o vía telefónica).

c) ¿En cuántos días le daremos respuesta a su solicitud?: su solicitud será resuelta en un plazo máximo de 15 días hábiles.

d) ¿Por qué medio le comunicaremos la respuesta a su solicitud?: Por el medio elegido por el titular en su solicitud de derechos ARCO (correo electrónico, dirección postal o vía telefónica).

e) ¿En qué medios se pueden proporcionar sus datos personales cuando se solicite el acceso?: Mediante documento de Word, Excel, audio o impreso con el costo correspondiente que represente su reproducción y envío en caso de que la entrega de los mismos se solicite a una dirección postal.

Los datos de contacto de la persona o departamento de datos personales que está a cargo de dar trámite a las solicitudes de derechos ARCO, son los siguientes:

a) Nombre de la persona o departamento de datos personales: "especificar nombre de la persona o nombre del departamento".

b) Domicilio: "Especificar domicilio completo, incluido C.P. y Entidad federativa".

c) Correo electrónico: ejemplo@dominio.com.

d) Número telefónico: “escribir número telefónico y extensión si existe”.

¿Como puedo revocar el consentimiento para el uso de mis datos personales?
Usted puede revocar el consentimiento que, en su caso, nos haya otorgado para el tratamiento de sus datos personales, en el momento que lo considere pertinente. Sin embargo, es importante que tenga en cuenta que no en todos los casos podremos atender su solicitud o concluir el uso de forma inmediata, ya que es posible que por alguna obligación legal requiramos seguir tratando sus datos personales.

Asimismo, usted deberá considerar que, para ciertos fines, la revocación de su consentimiento implicará que no le podamos seguir prestando el servicio que nos solicitó, o la conclusión de su relación con nosotros.

Para revocar su consentimiento deberá presentar el formulario de solicitud de derechos ARCO, solicitud por escrito o de manera verbal a través de los siguientes medios:

a) Mediante correo electrónico al correo ejemplo@dominio.com.
b) Mediante escrito libre en el domicilio del responsable, señalado con anterioridad.
c) De manera verbal en el domicilio del responsable.

¿Cómo puede limitar el uso o divulgación de su información personal?
Usted podrá limitar el uso de sus datos personales mediante el llenado y envío del formulario de solicitud de derechos ARCO, marcando la opción correspondiente, a través de los siguientes medios:

d) Mediante correo electrónico al correo ejemplo@dominio.com.
e) Mediante escrito libre en el domicilio del responsable, señalado con anterioridad.
f) De manera verbal en el domicilio del responsable.

Asimismo, usted se podrá inscribir a los siguientes registros, en caso de que no desee obtener publicidad de nuestra parte:

Registro Público para Evitar Publicidad, para mayor información consulte el portal de *Internet* de la PROFECO en la URL https://repep.profeco.gob.mx/

¿Cómo puede conocer los cambios en este aviso de privacidad?

El presente aviso de privacidad puede sufrir modificaciones, cambios o actualizaciones derivadas de nuevos requerimientos legales; de nuestras propias necesidades por los productos o servicios que ofrecemos; de nuestras prácticas de privacidad; de cambios en nuestro modelo de negocio, o por otras causas.

Nos comprometemos a mantenerlo informado sobre los cambios que pueda sufrir el presente aviso de privacidad, a través del enlace *"especificar la URL donde se publicará el aviso de privacidad actualizado"*, el cual le pedimos revise constante mente para verificar la fecha de actualización, donde también se adicionará un consecutivo de revisión a manera de control de cambios.

**Fecha de actualización: dd/mm/aaaa Rev. 01.**

El aviso de privacidad, además de cumplir con el principio de información, también debe garantizar el cumplimiento de los principios de proporcionalidad, finalidad, consentimiento, licitud, calidad, responsabilidad y lealtad, en ese sentido, ¿cómo podemos asegurar que el aviso de privacidad propuesto cumple con los principios mencionados?. A continuación, se explica de qué manera se cumple con ello en el aviso de privacidad, así como las medidas adicionales a implementar para el cumplimiento en la práctica del tratamiento de los datos personales.

Respecto al cumplimiento de la proporcionalidad, en el aviso de privacidad se enlistan los datos que se recolectan del titular, estos deben ser los mínimos necesarios para cumplir con las obligaciones contractuales del contrato jurídico entre el responsable y el titular. De tal manera que, si el titular se percata de que se recolectan datos excesivos para finalidades adicionales a las informadas en el aviso de privacidad, podrá ejercer sus derechos ante el responsable y si este no atiende a su solicitud, podrá iniciar un Procedimiento de Protección de Derechos ante el INAI.

Por su parte, el principio de finalidad se divide en dos partes, finalidad primaria y finalidad secundaria. La primaria es aquella necesaria para el cumplimiento de la obligación contractual entre el titular y el responsable, y la oposición al tratamiento de los datos para dicha finalidad supondría la cancelación de dicho contrato, mientras la Ley no establezca restricciones para la oposición.

La finalidad secundaria es aquella que no es necesaria para el cumplimiento de la obligación contraída entre el titular y el responsable, por tanto, el titular de los datos podrá oponerse a esa finalidad secundaria, y el responsable deberá establecer mecanismos en el aviso de privacidad para recolectar la manifestación de oposición, cuando así lo desee el titular de los datos.

El responsable no puede ni debe, usar los datos para finalidades que no sean compatibles con las finalidades informadas, es decir, si en el aviso de privacidad solo se informa que la finalidad del tratamiento es para realizar el cobro del producto o servicio y para el envío al domicilio del cliente, no tiene permitido hacer el envío de publicidad al correo electrónico o al domicilio del titular, en cuyo caso el titular podrá ejercer su derecho para limitar el uso y/o cancelar sus datos.

El principio de consentimiento se cumple al momento de informar sobre los datos que se recolectan, las finalidades y las condiciones del tratamiento, en ese sentido si el titular no manifiesta oposición a lo establecido en el aviso de privacidad, ni hace uso de los mecanismos implementados para oponerse al tratamiento, se presupone que consciente el tratamiento de sus datos de manera informada.

En cuanto a la licitud del tratamiento, el reglamento de la Ley, en el artículo 10 establece que “el principio de licitud obliga al responsable a que el tratamiento sea con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional”. En ese sentido, se obliga al cumplimiento de cada uno de los principios, implementar medidas de seguridad para garantizar la confidencialidad, proporcionar guías de apoyo para los titulares y a la observancia de la legislación internacional aplicable, en este caso, aplica el *Reglamento General de Protección de Datos del Consejo de Europa.*

En lo que refiere a la calidad de los datos, el aviso de privacidad cumple con informar el procedimiento para la rectificación, cuando estos no sean correctos o no

se encuentren actualizados. Cabe señalar que, no contar con los datos actualizados puede repercutir en la vida del titular, y en consecuencia, hacerse acreedores de una sanción, por ello, es importante recolectar los datos directamente del titular y establecer un procedimiento para que los mantenga actualizados.

En el aviso de privacidad se cumple con el principio de lealtad al no utilizar medios engañosos para la recolección de los datos, e informando claramente cuál será el tratamiento de los mismos, este principio supone que el responsable no defraudará la confianza que el titular haya depositado en él. Adicionalmente, este principio genera confianza en los clientes y repercute positivamente en la imagen de la empresa.

### *4.3.2. Guía para el ejercicio de los derechos ARCO*

Es importante tener en cuenta que para cumplir con lo establecido en el artículo 90 del Reglamento de la Ley, el responsable debe poner a disposición del titular los medios que considere pertinentes para facilitar el ejercicio de los derechos ARCO, para tal efecto se presenta un formulario mediante el cual, el titular de los datos podrá ejercer los derechos de acceso, rectificación, cancelación y oposición, acorde a lo establecido en el artículo 29 de la Ley.

Dicho formulario deberá ser referenciado en el aviso de privacidad, en el apartado del ejercicio de los derechos ARCO, así como la guía de usuario para el llenado de dicho formulario, de esta manera se cumple con lo establecido en el artículo 90 del reglamento.

A continuación, en la figura 4.2 se presenta la propuesta de formulario para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, así como limitar el uso o divulgación de los mismos y revocar el consentimiento, con las únicas limitantes que supone la Ley para cada uno de los casos.

Logotipo de la empresa

**DEPARTAMENTO DE DATOS PERSONALES**

*FORMULARIO PARA EL EJERCICIO DE DERECHOS ARCO, REVOCACIÓN DEL CONSENTIMIENTO Y/O LIMITACIÓN DE USO O DIVULGACIÓN DE DATOS PERSONALES*

• El presente formulario deberá ser llenado por el usuario titular de los datos personales o bien por su representante legal.
• Es indispensable que nos proporcione toda la información que se requiere a través de este formulario, ya que sólo de esa forma podremos verificar su identidad y estaremos en posibilidades de atender su solicitud.
• Favor de proporcionar la información sin abreviaturas.

**DATOS PERSONALES DEL TITULAR**

**Nombre** _____ **Apellido Paterno** _____ **Apellido Materno** _____

Elija el medio de contacto de su preferencia ☐ Correo electrónico ☐ Teléfono ☐ Domicilio postal

Especificar medio de contacto: _____

**DATOS DEL REPRESENTANTE LEGAL (CUANDO APLIQUE)**

Este apartado solo deberá ser llenado en caso de que, quien realice el tramite del ejercicio del los derechos ARCO, sea el representante legal, en cuyo caso, deberá adjuntar la documentación que se solicita en el apartado de documentos requeridos.

**Nombre** _____ **Apellido Paterno** _____ **Apellido Materno** _____

**IMPORTANTE:** Favor de acompañar la documentación que acredite la representación del titular en términos de ley mediante instrumento público o carta poder simple firmada ante dos testigos.

**TIPO DE SOLICITUD**

☐ Acceso ☐ Rectificación ☐ Cancelación ☐ Oposición
☐ Revocación ☐ Limitación del uso o divulgación

Favor de describir brevemente su solicitud:

| |
|---|
| |

Favor de describir clara y precisamente los datos personales respecto de los que se busca ejercer alguno de los derechos señalados anteriormente:

| |
|---|
| |

Marque el documento oficial que acompaña su solicitud y adjunte copia electrónica del mismo

☐ INE ☐ Cedula profesional ☐ Pasaporte
☐ Licencia de manejo ☐ Actad de nacimiento ☐ FM2, FM3 (documento migratorio vigente)

Los datos personales que nos proporciona a través de este formulario tienen como único objetivo el verificar la identidad del titular o de su representante legal y resguardar la seguridad de los mismos.

Figura 4.2. Formulario para el ejercicio de los derechos ARCO
*Fuente: Elaboración propia*

Respecto al llenado del formulario, es importante que el titular de los datos cuente con una guía para el correcto llenado del mismo, para ello, se debe poner a disposición en el aviso de privacidad la URL a la guía, en este caso la guía se adiciona al formulario de solicitud de derechos ARCO para que el titular pueda verla al momento de llenar el formulario. A continuación, se presenta una propuesta de guía para el llenado del formulario en la figura 4.3.

**INSTRUCCIONES DE LLENADO:**

A) Es obligatorio llenar los campos de los datos del titular, así como el medio de su elección de contacto

B) Los datos del representante legal solo se proporcionan en caso de que el tramite lo haga el representante, en nombre del titular, para ello debe adjuntar a la solicitud, el documento que acredite su personalidad como representante. El medio de contacto se tomará el elegido en el apartado de los datos del titular.

C) Debe marcar con una X el tipo de solicitud, además, debe tener en cuenta que por la natiraleza de cada uno de los derechos que puede ejercer, no se pueden ejercer de manera simultanea, por ello, debe marcar solo un tipo de solicitud.

D) En la descripción de la solicitud, especifíque claramente, por ejemplo: "ME opongo al tratamiento de mis datos personales para fines publicitarios"

E) En la descripción de los datos respecto a los que desea ejercer su derecho, especifíque claramente, por ejemplo: Me han estado haciendo llamadas a mi télefono celular, o me han estado mandando publicidad a mi correo electrónico"

F) Finalmente, debe marcar con qué documento está acreditando su identidad y adjuntar el documento marcado en el formulario para verificar su identidad.

Figura 4.3. Instrucciones de llenado del formulario de solicitud de derechos ARCO
*Fuente: Elaboración propia*

### *4.3.3. Designación del departamento de datos personales*

En cumplimiento a lo establecido en el artículo 30 de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* el responsable debe designar a una persona o departamento –según lo considere necesario–, responsable de los datos personales, así como de dar seguimiento a las solicitudes de derechos ARCO.

Para ello, es necesario que la persona responsable tenga conocimientos de derecho y protección de datos[209], además de conocimiento sobre tecnologías.

En tal sentido, la persona responsable de los datos personales o quien esté al frente del departamento, será el sujeto cualificado del que se habla en el segundo capítulo, por ende, es la persona que debe coadyuvar en la capacitación, en el diseño e implementación de medidas de seguridad, en conjunto con el departamento de tecnologías de la información, así como la resolución de controversias que se puedan suscitar en torno al tratamiento de los datos.

En consecuencia, el departamento de datos personales debe tener la jerarquía de dirección o en su caso fungir como un departamento de staff. En todo caso, la persona responsable de los datos personales, debe contar con el rango jerárquico que lo faculte para poder imponer procedimientos, políticas y estándares que favorezcan el respeto de la privacidad de los titulares, en torno al tratamiento que de los datos se haga al interior de la empresa.

Por consiguiente, el desarrollo del documento de seguridad, deberá realizarse entre la persona o departamento de datos personales y el departamento de tecnologías de la información, de tal manera que en dicho documento se plasmen los procesos y las responsabilidades de cada interviniente en el tratamiento de los datos, y con la intención de que se apoyen ambas disciplinas –derecho y tecnologías–, para dotar de seguridad jurídica y técnica los datos tratados y favorecer el ejercicio de los derechos de los titulares. Poniendo siempre como elemento central a la persona humana y su integridad física, moral y patrimonial.

### *4.3.4. Parámetros generales del inventario de datos personales*

La obligación de realizar un inventario de datos personales se fundamenta en el artículo 61 del reglamento de la Ley; es un elemento de suma importancia que debe contener el documento de seguridad, ya que es la base para el análisis del riesgo inherente a los datos, actividad que el citado artículo obliga a realizar para determinar las medidas de seguridad adecuadas para la protección de los datos.

---

[209] *Cfr.* Agencia Española de Protección de Datos, *Esquema de certificación de delegados de protección de datos de la agencia española de protección de datos (esquema aepd-dpd),* 2019, https://www.aepd.es/sites/default/files/2020-07/esquema-aepd-dpd.pdf. Consultado: 21/06/2020.

A manera de ejemplo, se presenta un inventario de datos personales tomando como referencia los lineamientos de la "Metodología de Análisis de Riesgo BAA"[210], en combinación con algunos elementos a criterio personal, con la intención de presentar de manera clara el procedimiento para el inventario de datos, aunque este procedimiento también puede realizarse en base a alguna otra metodología de análisis de riesgos, como por ejemplo Octave Allegro, ITIL o ISO.

El motivo por el cual se utiliza la metodología BAA, es debido a que es el documento desarrollado por el órgano garante en México, y se presume que el apego a dicha metodología garantiza el cumplimiento de la Ley, en cuanto a detección de riesgos y la implementación de medidas de seguridad se refiere.

A continuación, se presenta le inventario de datos personales, el cual, parte del supuesto de una micro empresa del sector comercial que se dedica a la venta al menudeo de artículos de vestir para dama y caballero. Tiene contratado un servicio de cómputo en la nube, donde almacena el sistema de comercio electrónico, así como la base de datos de clientes, inventario y sistema de nómina.

En el inventario de datos, es necesario conocer los sistemas que tiene la empresa, los tipos de datos que se almacenan en cada uno de ellos, la sensibilidad por tipo de dato, el riesgo inherente por tipo de dato, la anonimidad de los datos –que tan difícil puede ser acceder de acuerdo al medio de almacenamiento y canal de comunicación–, así como la cantidad de los datos por cada tipo de sensibilidad.

Cabe precisar que se debe entender que los datos de identificación son de sensibilidad baja y su riesgo inherente será bajo; los datos financieros y/o patrimoniales y los de geolocalización –domicilio físico– son de sensibilidad media y su riesgo inherente es medio, mientras que los de identificación son de sensibilidad baja y riesgo inherente bajos.

Además, al analizar los patrones de compra se puede determinar los gustos de cada cliente –datos sensibles– que si bien, no son almacenados, son determinables mediante la información almacenada. También es importante señalar que la

[210] INAI, *Metodología de Análisis de Riesgos BAA,* 2015, http://inicio.ifai.org.mx/DocumentosdeInteres/Metodolog%C3%ADa_de_An%C3%A1lisis_de_Riesgo_BAA(Junio2015).pdf. Consultado: 21/06/2020.

combinación en algunos datos puede dar como resultado un riesgo inherente reforzado, mientras que, de los datos almacenados, ninguno da como resultado un riesgo inherente alto.

Para tal efecto, se toma en cuenta que los datos que se recolectan de los clientes son los necesarios para la facturación, envío de los productos al domicilio, género, número de tarjeta de pago. Al realizar el pago interviene un tercero para realizar la transacción del dinero, el cual tiene su servidor en Estados Unidos de América, el proveedor del servicio de nube es Amazon, además, también tiene una tienda física en México, en donde se realiza venta al público y la información de las transacciones se maneja con los mismos sistemas en la nube, y para las transacciones se utiliza la terminal y el sistema del banco contratado.

### *4.3.5. Guía para la elaboración del inventario de datos*

De acuerdo al planteamiento, los datos que se recolectan varían de acuerdo a la modalidad de las ventas, primero se debe crear una cuenta de usuario en el sistema de e-commerce, en donde se solicitan los datos de nombre, correo electrónico, domicilio completo y teléfono de contacto, estos datos son los que se utilizarán para identificar a la persona y enviar los productos al domicilio.

Adicionalmente se cuenta con el sistema de facturación, en el cual se recolectan los datos de los clientes para fines de emitir las facturas correspondientes a sus compras, para tal efecto se recolecta el nombre, RFC, domicilio (calle, número, C.P., ciudad, estado, país), teléfono de contacto y correo electrónico. Estos datos se recolectan independientemente de si la venta se realiza en línea o en el local físico.

En lo que respecta a las transacciones de dinero, los datos que se recolectan por la empresa que se contrata para dicha operación, son: número de tarjeta, nombre completo, domicilio completo la IP física del dispositivo y la ubicación desde donde se realiza la transacción. Es preciso recordar que estos datos no los almacena la empresa del responsable, sino el tercero que se ha contratado para realizar las transacciones, sin embargo, la responsabilidad del adecuado tratamiento es de la empresa.

Asimismo, en el sistema de nómina se conservan datos relacionados a los empleados, tales como nombre, domicilio, teléfono, correo electrónico, número de cuenta bancaria, horario laboral, cargo desempeñado y salario quincenal.

Cada tipo de dato tiene un riesgo inherente acorde al beneficio que representa para los atacantes de acuerdo a su sensibilidad; acorde a los tipos de datos que se almacenan en este supuesto, la tabla de riesgo inherente a los datos por cada sistema utilizado, queda representado en la tabla 4.1 de la siguiente manera:

| Sistema | Tipo de dato | Nivel de riesgo inherente |
|---|---|---|
| Nómina | Ubicación y contacto | Medio |
| | Financieros | Medio |
| | Identificación | Bajo |
| | Autenticación | Medio |
| Facturación | Identificación | Medio |
| | Ubicación y Contacto | Medio |
| | Financieros | Medio |
| e-commerce | Identificación | Bajo |
| | Autenticación | Medio |
| Transacciones | Autenticación | Bajo |

Tabla 4.1. Identificación del nivel de riesgo inherente por tipo de dato
*Fuente: Retomada de la Metodología para análisis de riesgo BAA, 2015, p. 4.*

Los datos de contacto y el domicilio del cliente son fundamentales en las ventas en línea, pues sin este dato no se le podría entregar el producto en la puerta de su casa, el conocimiento de estos datos *per se,* no representa un riesgo inherente alto. Sin embargo, al conjuntarlo con el dato de la tarjeta de crédito incrementa el riesgo inherente a un nivel reforzado, de tal manera que, si se relaciona con el beneficio, la anonimidad y la accesibilidad, resulta ser información bastante delicada por el riesgo inherente que representa para el titular, motivo por el cual se debe evitar en la medida de lo posible que la empresa almacene los números de tarjeta de los clientes.

Por consiguiente, se especula que la empresa almacena en sistemas propietarios alojados en una nube, los datos de los empleados para el pago de salarios, el inventario de mercancías en el sistema de e-commerce que almacena los usuarios

administradores del mismo, los datos de autenticación de los clientes del servicio en línea, así como los datos de los clientes para facturación y envió de productos. Mientras que los datos bancarios son tratados por un tercero encargado, acción que se debe informar en el aviso de privacidad en el apartado dedicado para ello.

De tal manera que el inventario de sistemas, la cantidad de registros y usuarios que pueden autenticarse para acceder a los mismos, queda como se ilustra en la tabla 4.2.

| Sistema | Ubicación | Registros | Responsable | Usuarios |
|---|---|---|---|---|
| Nómina | Nube de Amazon | 50 | Empresa | 5 |
| e-commerce | Nube de Amazon | 250,000 | Empresa | 250,000 |
| Facturación | Nube de Amazon | 450,000 | Empresa | 250,000 |
| Transacciones | Tercero | N/A | Tercero | 1 |

Tabla 4.2. Inventario de sistemas y volumen de datos
*Fuente: Elaboración propia*

Las áreas de la empresa que tienen acceso a los sistemas donde se almacenan los datos personales son los siguientes: A los datos del cliente para fines de facturación, tiene acceso el departamento de contabilidad; a los datos de autenticación de los clientes en el sistema de e-commerce tienen acceso dos personas del departamento de sistemas y cinco del departamento de ventas; al sistema de nómina tiene acceso el departamento de recursos humanos, contabilidad y administración, mientras que al sistema de transacciones solo tiene acceso el tercero contratado para tales efectos.

### *4.3.6. Parámetros generales del análisis de riesgo*

Una vez identificado lo anterior, se procede a la identificación del riesgo latente, el cual se obtiene de la identificación de riesgo por tipo de dato, más la accesibilidad, más la anonimidad, para este efecto, la metodología establece las siguientes métricas para la representación del volumen de datos: “<500: datos de hasta 500 personas; <5k: datos entre 501 hasta 5,000 personas; <50k: datos de 5,001 hasta

50,000 personas; <500k: datos de 50,001 hasta 500,000 personas y >500k: datos de más de 500,000 personas"[211].

Tomando en consideración las métricas de la metodología, a continuación, se presenta el análisis de riesgo inherente al beneficio para cada uno de los sistemas, comenzando con el de nóminas en la tabla 4.3, al cual se le dará acceso solo a dos personas del departamento de contabilidad, dos personas de recursos humanos y una persona de administración, dando un total de cinco personas con claves de autenticación para dicho sistema, mientras que la cantidad de registros corresponde a cada uno de los empleados de la empresa, y de exempleados por un periodo de un año posterior a la separación del contrato laboral.

| **Sistema de nómina** | | | | | | |
|---|---|---|---|---|---|---|
| **Tipo de dato** | **Nivel de riesgo inherente** | **Volumen de titulares** | | | | |
| | | **<500** | **<5k** | **<50k** | **<500k** | **>500k** |
| Ubicación y | Medio | 1 | 1 | 2 | 3 | 3 |
| Financieros | Medio | 1 | 1 | 2 | 3 | 3 |
| Autenticación | Medio | 1 | 1 | 2 | 3 | 3 |
| Identificación | Bajo | 1 | 1 | 1 | 1 | 1 |

Tabla 4.3. Nivel de riesgo inherente por volumen de datos en el sistema de nómina
*Fuente: Elaboración propia basado en la metodología de análisis de riesgo BAA, 2015, p. 9.*

Al sistema de e-comerce pueden acceder los clientes que se han registrado en línea, así como dos personas del departamento de sistemas, quienes tienen permisos de administración sobre la información que se almacena respecto a los clientes, y cinco personas del departamento de ventas encargadas de realizar el envío de los productos a los clientes, dando como resultado la tabla 4.4 de riesgo inherente que se muestra a continuación.

| **Sistema de e-commerce** | | | | | | |
|---|---|---|---|---|---|---|
| **Tipo de dato** | **Nivel de riesgo inherente** | **Volumen de titulares** | | | | |
| | | **<500** | **<5k** | **<50k** | **<500k** | **>500k** |
| Autenticación | Medio | 1 | 1 | 2 | 3 | 3 |
| Identificación | Bajo | 1 | 1 | 1 | 1 | 1 |

Tabla 4.4. Nivel de riesgo inherente por volumen de datos en el sistema de e-commerce
*Fuente: Elaboración propia basado en la metodología de análisis de riesgo BAA, 2015, p. 9.*

[211] *Ibiden,* p. 6.

Respecto al sistema de facturación, el volumen de datos se toma en relación al total de registro del sistema, correspondiente a los clientes, dando como resultado la tabla 4.5 de riesgo inherente que se muestra en seguida.

| Sistema de facturación | | | | | | |
|---|---|---|---|---|---|---|
| **Tipo de dato** | **Nivel de riesgo inherente** | **Volumen de titulares** | | | | |
| | | **<500** | **<5k** | **<50k** | **<500k** | **>500k** |
| Financieros | Medio | 1 | 1 | 2 | 3 | 3 |
| Ubicación y | Medio | 1 | 1 | 2 | 3 | 3 |
| Identificación | Medio | 1 | 1 | 2 | 3 | 3 |

Tabla 4.5. Nivel de riesgo inherente por volumen de datos en el sistema de e-commerce
*Fuente: Elaboración propia basado en la metodología de análisis de riesgo BAA, 2015, p. 9.*

En relación al sistema de transacciones, el tercero contratado para tal efecto ha implementado las medidas de seguridad pertinentes, en lo que respecta a la empresa solo cuenta con un usuario de autenticación para realizar las transacciones, dando como riesgo inherente el resultado la tabla 4.6.

| Sistema de transacciones | | | | | | |
|---|---|---|---|---|---|---|
| **Tipo de dato** | **Nivel de riesgo inherente** | **Volumen de titulares** | | | | |
| | | **<500** | **<5k** | **<50k** | **<500k** | **>500k** |
| Autenticación | Medio | 1 | 1 | 2 | 3 | 3 |

Tabla 4.6. Nivel de riesgo inherente por volumen de datos en el sistema de e-commerce
*Fuente: Elaboración propia basado en la metodología de análisis de riesgo BAA, 2015, p. 9.*

A continuación, se presenta el nivel de riesgo por tipo de acceso en un intervalo de tiempo de 24 horas, respecto a este parámetro se consideran los usuarios con permisos de autenticación al mismo y no el volumen de datos, por tanto, el factor de riesgo inherente a la accesibilidad, da como resultado la siguiente tabla 4.7, de acuerdo a los sistemas identificados.

| **Sistema** | **Tipo de dato** | **Accesibilidad** | **Nivel de riesgo** |
|---|---|---|---|
| *Nómina* | Ubicación y contacto | < 20 | 1 |
| | Financieros | <20 | 1 |
| | Identificación | <20 | 1 |

| Sistema | Tipo de dato | Accesibilidad | Nivel de riesgo |
|---|---|---|---|
| | Autenticación | <20 | 1 |
| *Facturación* | Identificación | >2,000 | 1 |
| | Ubicación y Contacto | >2,000 | 3 |
| | Financieros | >2,000 | 3 |
| *e-commerce* | Identificación | >2,000 | 1 |
| | Autenticación | >2,000 | 3 |
| *Transacciones* | Autenticación | <20 | 1 |

Tabla 4.7. Nivel de accesibilidad para el atacante
*Fuente. Elaboración propia basado en la metodología de análisis de riegos BAA, 2015.*

De igual manera se requiere tener conocimiento del nivel de anonimidad del atacante, este se determina en función de los medios de acceso a los sistemas, de tal manera que cuando se trabaja con sistema de cómputo en la nube, la anonimidad para el atacante es alta, puesto que los servidores donde se alojan los sistemas deberán permanecer en línea 24/7/365, y accesibles desde cualquier parte del mundo mediante *Internet,* de tal manera que la tabla 4.8 correspondiente al riesgo por tipo de accesibilidad queda de la siguiente manera.

| Sistema | Entorno | Nivel de anonimidad |
|---|---|---|
| Nómina | Red interna | 2 |
| | Internet | 5 |
| e-commerce | Red interna | 2 |
| | Internet | 5 |
| Facturación | Red interna | 2 |
| | Internet | 5 |
| Transacciones | Red interna | 2 |
| | Internet | 5 |

Tabla 4.8. Nivel de anonimidad para el atacante para cada sistema
*Fuente: Elaboración propia, basado en la metodología de análisis de riesgo BAA, 2015.*

En este caso solo se toma en cuenta la red interna y el *Internet,* puesto que los accesos que realicen por parte del personal de la empresa con fines administrativos y de operación del negocio, provienen de la red del local físico, la cual puede estar

expuesta mediante algún ataque como el que se muestra en el capítulo tercero, que puede originar la vulneración de los sistemas almacenados en la nube.

Así entonces, el riesgo por tipo de dato se obtiene del riesgo inherente por el volumen de datos, por tanto, según los parámetros identificados anteriormente, queda como se muestra en la tabla 4.9, de acuerdo a cada uno de los sistemas de tratamiento de datos identificados.

| **Sistema** | **Tipo de dato** | **Nivel de riesgo inherente** | | **Riesgo por tipo de dato** |
|---|---|---|---|---|
| Nómina | Ubicación y contacto | Medio | 1*50 | 50 |
| | Financieros | Medio | 1*20 | 20 |
| | Identificación | Bajo | 1*50 | 50 |
| | Autenticación | Medio | 1*5 | 5 |
| Facturación | Identificación | Medio | 3*450,000 | 1,350,000 |
| | Ubicación y Contacto | Medio | 3*450,000 | 1,350,000 |
| | Financieros | Medio | 3*450,000 | 1,350,000 |
| e-commerce | Identificación | Bajo | 3*250,000 | 750,000 |
| | Autenticación | Medio | 1*250,000 | 250,000 |
| Transacciones | Autenticación | Bajo | 1*1 | 1 |

Tabla 4.9. Tabla de riesgo por tipo de dato
*Fuente: Elaboración propia*

Una vez determinado el riesgo, se estará en condiciones de proceder a determinar las medidas de seguridad a implementar, para ello, tomando como referencia la metodología en cuestión, se presenta la metodología para determinar las medidas de seguridad a implementar.

*A. Detección de medidas de seguridad*

De acuerdo a los parámetros de la metodología BAA, primero se deben detectar las medidas de seguridad administrativas, para lo cual, se proponen cinco tablas que representan las medidas de seguridad detectadas acorde al nivel de riesgo por tipo de dato, para este caso se retoma el nivel de riesgo detectado en la tabla 4.3, y en relación al entorno de acceso, se determinan las siguientes medidas de seguridad administrativas.

La primera tabla corresponde a los datos de ubicación en el cual se detectó un nivel de riesgo inherente medio; la segunda corresponde a los datos patrimoniales con un nivel de riesgo inherente medio; la tercera corresponde a los datos de autenticación de los usuarios cuando acceden a su perfil de clientes y, por último, la cuarta tabla corresponde a los datos de identificación, tanto de los clientes, como de los empleados de la empresa.

Identificando las tablas de control, se identifica de acuerdo al tipo de dato y al entorno de acceso, las medidas de seguridad para cada tipo de dato, dando como resultado la siguiente tabla 4.10, correspondiente a las medidas de seguridad para el tipo de dato 1, cabe resaltar que el color más fuerte hace referencia al volumen de datos, mientras que el color más suave corresponde al nivel de riesgo bajo.

| | | **Riesgo por tipo de dato 1. Datos de** | | | |
|---|---|---|---|---|---|
| | | **Medidas administrativas aplicables AD-3** | | | |
| Entornos de acceso | Internet | CB | CB | CB | CB |
| | Red terceros | CB | CB | CB | CB |
| | | ≤ 20 | ≤ 200 | **≤ 2,000** | **> 2,000** |
| | | Cantidad de Accesos / Personas | | | |

Tabla 4.10. Medidas de seguridad administrativa para datos de identificación
*Fuente: Elaboración propia*

De igual manera, la tabla 4.11 identifica las medidas de seguridad de acuerdo al tipo de dato 3, que en relación al volumen de datos se entiende que las medidas de seguridad deberán ser aplicadas a la red interna, así como a los sistemas de acuerdo al requerimiento para protegerse de entornos de alta anonimidad.

| | | **Riesgo por tipo de dato 3. Datos de ubicación** | | | |
|---|---|---|---|---|---|
| | | **Medidas administrativas aplicables AD-3** | | | |
| Entornos de acceso | Internet | RI-2, AD-3, DMZ-2 | RI-2, AD-3, DMZ-2 | RI-2, AD-3, DMZ-2 | RI-2, AD-3, DMZ-2 |
| | Red interna | RI-2, AD-3 | RI-2, AD-3 | RI-2, AD-3 | RI-2, AD-3 |
| | | ≤ 20 | ≤ 200 | **≤ 2,000** | **> 2,000** |

| | | Cantidad de Accesos / Personas |
|---|---|---|

Tabla 4.11. Medidas de seguridad administrativas para datos de ubicación
*Fuente: Elaboración propia*

Respecto a los datos financieros, se estiman las medidas de seguridad acorde al volumen de datos, dando como resultado un nivel de seguridad acorde a la cantidad de titulares de los que se conservan datos bancarios para las transacciones de los salarios, tal como se observa en la siguiente tabla 4.12.

| | | **Riesgo por tipo de dato 3. Datos financieros** | | | |
|---|---|---|---|---|---|
| | | **Medidas administrativas aplicables AD-3** | | | |
| Entornos de acceso | Internet | RI-2, AD-3, DMZ-2 | RI-2, AD-3, DMZ-2 | RI-2, AD-3, DMZ-2 | RI-2, AD-3, DMZ-2 |
| | Red interna | RI-2, AD-3 | RI-2, AD-3 | RI-2, AD-3 | RI-2, AD-3 |
| | | ≤ 20 | ≤ 200 | **≤ 2,000** | **> 2,000** |
| | | Cantidad de Accesos / Personas | | | |

Tabla 4.12. Medidas de seguridad administrativas para datos patrimoniales
*Fuente: Elaboración propia*

Los datos de autenticación corresponden a los usuarios de acceso a los sistemas, que pertenecen a los clientes del servicio de ventas en línea o del personal administrativo, en cualquiera de los casos los entornos de acceso recaen sobre *Internet,* por ende, el riesgo para este tipo de dato se observa en la tabla 4.13.

| | | **Riesgo por tipo de dato 3. Datos de** | | | |
|---|---|---|---|---|---|
| | | **Medidas administrativas aplicables AD-3** | | | |
| Entornos de acceso | Internet | RI-2, AD-3, DMZ-2 | RI-2, AD-3, DMZ-2 | RI-2, AD-3, DMZ-2 | RI-2, AD-3, DMZ-2 |
| | Red interna | RI-2, AD-3 | RI-2, AD-3 | RI-2, AD-3 | RI-2, AD-3 |
| | | ≤ 20 | ≤ 200 | **≤ 2,000** | **> 2,000** |
| | | Cantidad de Accesos / Personas | | | |

Tabla 4.13. Medidas de seguridad administrativa para datos de autenticación
*Fuente: Elaboración propia*

Respecto a los datos de ubicación y contacto, son los que pueden ser accedidos tanto por cada uno de los usuarios para actualizar o modificar su información personal en el perfil de la tienda en línea, además de ser conocidos para el personal de ventas, quien usará esta información para el envío de los productos, de tal manera que, se requiere tener medidas de seguridad implementadas para prevenir ataques mediante este vector de riesgo que se muestra en la tabla 4.14.

| | | **Riesgo por tipo de dato 3. Ubicación y contacto** | | | |
|---|---|---|---|---|---|
| | | **Medidas administrativas aplicables AD-3** | | | |
| Entornos de acceso | Internet | RI-2, AD-3, DMZ-2 | RI-2, AD-3, DMZ-2 | RI-2, AD-3, DMZ-2 | RI-2, AD-3, DMZ-2 |
| | Red interna | RI-2, AD-3 | RI-2, AD-3 | RI-2, AD-3 | RI-2, AD-3 |
| | | ≤ 20 | ≤ 200 | **≤ 2,000** | **> 2,000** |
| | | Cantidad de Accesos / Personas | | | |

Tabla 4.14. Medidas de seguridad administrativa para datos de ubicación y contacto
*Fuente: Elaboración propia*

De acuerdo a las tablas anteriores, se puede determinar en la primera tabla que es necesario aplicar medidas de seguridad para entornos de alta anonimidad y acorde al nivel de riesgo inherente detectado en la tabla 4.3. Lo mismo ocurre con la tabla 4.8 y 4.9, con la única variante del volumen de datos en la tabla correspondiente a los datos patrimoniales, ya que estos solo se recolectan de los empleados para poder realizar las transferencias por el pago de salarios.

a. Recomendaciones para las medidas de seguridad administrativa

Las medidas administrativas tienen como objetivo tener control sobre las acciones que se deben realizar para mitigar los riesgos detectados, en tal sentido, la metodología de análisis de riesgo BAA, contempla una serie de controles para cada tabla de riesgo por tipo de datos, no obstante, las medidas de seguridad deberán ser adecuadas a cada organización, al entorno de acceso y al factor de beneficio para los atacantes.

A manera de guía para las medidas de seguridad administrativas se recomienda que el responsable diseñe controles para:

- Administración de usuarios: Control que debe contemplar el ciclo de vida de los usuarios, la periodicidad del cambio de contraseñas, las medidas de resguardo por los usuarios para que no sean conocidos por terceros ajenos o no autorizados, así como los niveles de acceso a los datos, para ello, se presenta una propuesta de política en el Anexo 1.
- Políticas de uso de correo electrónico: Se recomienda que el responsable elabore las políticas para el uso de correo electrónico, en las que se debe especificar la propiedad el mismo, así como de la información que mediante este se envíe, las responsabilidades en materia de datos personales, las limitantes para su uso, las facultades del responsable para auditar el contenido, el acuerdo de confidencialidad de la información, entre otras que se consideren necesarias, a manera de ejemplo se presenta el Anexo 2 para dichas políticas.
- Políticas de uso de equipo de cómputo: En este documento se debe especificar las medidas de seguridad que debe tener en cuenta el usuario, la propiedad de la información y del equipo, las restricciones de instalación de software, el resguardo de las claves de usuario, las sanciones por negligencia, entre otras que se consideren pertinentes, a manera de propuesta se presenta el Anexo 3.
- Destrucción segura de datos personales: El responsable deberá implementar medidas de destrucción segura de datos personales, por ejemplo, el uso obligatorio de trituradoras para desechar papeles con datos personales o de valor para la empresa, procedimientos para la destrucción segura de información contenida en medios magnéticos como memorias USB, discos duros, cintas magnéticas, etc.
- Capacitación: El responsable deberá diseñar planes de capacitación para todo el personal, los cuales tendrán la intención de concientizar a los trabajadores sobre la importancia de proteger debidamente los datos personales, el respeto del derecho a la protección de los datos personales, así como para la atención de los procedimientos de derechos ARCO. Para

este caso, el Anexo 4 presenta un plan de capacitación para el personal interno.

b. Medidas de seguridad técnicas

Las medidas de seguridad técnicas que la ley exige al responsable del tratamiento de los datos, se desprenden en buena medida del análisis de riesgo. No obstante, las medidas de seguridad pueden ser mayores, e incluso se recomienda que vallan un poco más allá de las que se consideran necesarias para mitigar los riesgos detectados.

En el caso del uso de los sistemas de cómputo en la nube, en donde se considera que el responsable solo ha contratado la infraestructura y la plataforma como servicios, la seguridad de los sistemas web corresponde a este, por lo que es recomendable que se implementen metodologías para el desarrollo seguro, tales como, *Microsoft Trustworthy Computing SDL*[212]*; CLASP (Comprehensive, Lightweight Application Security Process)*[213]*; Wrinting Source Code*[214] y/o *Oracle Software Security Assurance*[215], por mencionar algunas, además de tener en cuenta la privacidad por diseño[216] del modelo canadiense para la protección de los datos personales y el respeto a los derechos de los titulares.

Puesto que en los servicios de nube la infraestructura física es administrada por los prestadores del servicio, el responsable no tendrá forma de administrar la seguridad física, motivo por el cual, no se contemplan dichas medidas en este trabajo como prioridad para mitigar el riesgo de los datos personales.

---

[212] Lipner, Steve, "The trustworthy computing security development lifecycle", *ResearchGate,* 2005, https://www.researchgate.net/publication/4115440_The_trustworthy_computing_security_development_lifecycle. Consultado: 22/06/2020.

[213] Secure Sofware, Inc., *The CLASP Application Security Process,* 2005, https://cwe.mitre.org/documents/sources/TheCLASPApplicationSecurityProcess.pdf. Consultado: 22/06/2020.

[214] Microsoft, *Writing Secure Code,* 2003, https://ptgmedia.pearsoncmg.com/images/9780735617223/samplepages/9780735617223.pdf. Consultado: 23/06/2020.

[215] Beaver, Kevin, Tips and Tricks Guide To Software Security Assurance, https://www.principlelogic.com/docs/Tips_and_Tricks_Guide_to_Software_Security_Assurance.pdf. Consultado: 23/06/2020.

[216] Cavoukian, Ann, *Privacy by Design,* 2006, https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf. Consultado: 23/06/2020.

Así entonces, el responsable, propietario de los sistemas que operan en la plataforma de nube, deberá enfocar sus esfuerzos en la resistencia de los sistemas ante ataques de fuerza bruta, confidencialidad de la información en tránsito mediante cifrado de la información, así como el rastreo de la actividad de los usuarios autorizados para el tratamiento de los datos, con la finalidad de conocer a detalle a que información se accedió, los movimientos que se realizaron y si el usuario estaba autorizado para realizar dichos movimientos.

Los usuarios autenticados deberán tener acceso solo al nivel que les corresponde, y no podrán conocer aquella información para la que como usuario del sistema no estén autorizados. Esto se logra mediante la implementación de políticas de usuario en el sistema para que, al momento de ingresar el usuario y contraseña, se detecten los permisos del usuario y se limite el acceso solo a lo estipulado para el nivel de usuario en cuestión.

Se recomienda tener usuarios de tipo administrador, que tendrán todos los permisos y podrán visualizar la totalidad de los datos, se recomienda que este tipo de usuarios se les habilite a los administradores de sistemas; usuarios directivos, los cuales tendrán acceso al sistema para monitorear y consultar información, su acceso está enfocado a los reportes y no al tratamiento de los datos *per se;* usuarios operadores, los cuales podrán capturar la información y solo aquella que les corresponda de acuerdo a las actividades desempeñadas; los programadores, analistas y diseñadores de bases de datos requieren tener todos los permisos para poder realizar las pruebas pertinentes antes de poner en producción los sistemas.

c. Análisis de brecha

Adicionalmente se debe realizar un análisis de brecha, el cual consta de la identificación de las medidas de seguridad faltantes para lograr mitigar los riesgos de manera eficiente. Para ello, se toman como referencia las medidas de seguridad actuales, y se determinan las acciones pertinentes para implementar las medidas faltantes.

En el caso que se plantea en este documento, se presupone que el responsable ha contratado una plataforma como servicio para montar los sistemas de nómina,

e-commerce, facturación y la conexión al sistema de transacciones, en tal sentido, el proveedor del servicio de nube proporciona la seguridad perimetral y de la plataforma, mientras que la seguridad que corresponde a los sistemas corre por cuenta del responsable.

Así entonces, de conformidad con el considerando 83 y el artículo 32, referente a la seguridad en el tratamiento establecido en el *Reglamento General de Protección de Datos del Consejo de Europa,* así como las medidas de seguridad establecidas en los artículos 19 y 20 e la Ley, el responsable debe implementar controles tecnológicos para garantizar la seguridad y confidencialidad de la información.

Es importante mencionar que cuando se hace uso de la tecnología para el tratamiento de datos personales y más aún, siendo tecnología de nube caracterizada por la ubicuidad, el tratamiento de los datos debe apegarse a los convenios y tratados internacionales, en este caso, para el tema de datos personales, México es parte firmante del convenio 108, mismo que obliga a la observancia del reglamento de protección de datos de Europa, por ende, para garantizar la seguridad en mayor medida, el responsable deberá implementar mecanismos de cifrado de la información.

Para el cifrado de los datos personales, se debe valorar la importancia en relación al riesgo detectado por tipo de dato, pues por lo regular el mecanismo de cifrado va a disminuir la velocidad de operación de los sistemas, motivo por el que no se recomienda cifrar la totalidad de la base de datos. Sin embargo, es recomendable cifrar aquellos datos que representen mayor beneficio para el atacante.

Un método de cifrado de datos en la recolección en línea, es mediante MD5 o SHA256, que al anteponerlo a la variable que contiene los datos a insertar en la base de datos, estos se enviarán cifrados a la base de datos y así permanecerán hasta que algún usuario, mediante la autenticación con su usuario y contraseña los consulte.

Este método de cifrado por lo regular se aplica para las contraseñas de usuario, sin embargo, parece pertinente aplicar el cifrado a los datos que puedan causar mayor perjuicio al titular, por ejemplo, datos financieros, datos de ubicación y/o de

contacto, mientras que los datos como el nombre y edad, no suponen un alto riesgo para la persona humana.

*4.3.7. Imposición de sanciones por incumplimiento a los principios de la Ley*

Es importante recalcar que, de no cumplir con los principios establecidos en la Ley, así como de sus demás disposiciones en materia de protección de datos personales, el responsable se puede hacer acreedor a una sanción económica, o a una pena de prisión de acuerdo a lo establecido en los artículos 64 y 65 de la Ley respectivamente.

En lo que respecta a las sanciones, se solicitó al INAI mediante la Plataforma Nacional de Transparencia, información correspondiente al total de sanciones emitidas en el último año, de esas sanciones cuantas fueron realmente cobradas por el Servicio de Administración Tributaria y cuantas habían sido impugnadas ante los tribunales correspondientes.

En su respuesta con número de oficio INAI/SPDP/DGPDS/292/20, informa al respecto que en el periodo que corresponde del 23 de junio de 2019 al 23 de junio de 2020 se han emitido "595 resoluciones en las que ha impuesto sanción a empresas por incumplimiento de alguno de los principios o disposiciones de la Ley […] de las cuales, 275 han sido impugnadas ante la autoridad administrativa y/o judicial"[217].

En relación a las multas cobradas, el instituto manifiesta que derivado del convenio de colaboración suscrito con el Servicio de Administración Tributaria, firmado el 9 de noviembre de 2015, "a fin de que esta última controle y lleve a cabo el cobro de las multas que se impongan a los sujetos regulados por la Ley"[218], las Administraciones Descentralizadas de Recaudación Fiscal de las Entidades del domicilio de las empresas sancionadas, son las encargadas de realizar el cobro de las sanciones.

Por tal motivo el instituto desconoce sobre el cumplimiento de las sanciones aplicadas, informando al respecto que de 2013 a 2018 solo se tiene el dato de trece

[217] INAI, *Oficio número INAI/SPDP/DGPDS/292/20,* 2020, en respuesta a la solicitud de información realizada mediante la Plataforma Nacional de Transparencia, p. 3.
[218] INAI, *Oficio…, Op Cit.* p. 3.

empresas que voluntariamente el Servicio de Administración Tributaria y/o las mismas empresas han informado al instituto sobre dicho cumplimiento, y adjunta la tabla 4.15 que muestra el nombre de la empresa y el monto de la multa pagada.

| AÑO | INFRACTOR | SECTOR | IMPORTE MULTA IMPUESTA | IMPORTE MULTA PAGADA |
|---|---|---|---|---|
| 2013 | BUHOLEGAL S. DE R.L. DE C.V. | SERVICIOS PROFESIONALES, CIENTÍFICOS Y TÉCNICOS | $20,399.00 | $20,399.00 |
| 2014 | CREACIONES TEXTILES DE MÉRIDA, S.A. DE C.V. | INDUSTRIAS MANUFACTURERAS | $129,520.00 | $131,269.00 |
| 2014 | BANCO MERCANTIL DEL NORTE, S.A., INSTITUCIÓN DE BANCA MÚLTIPLE, GRUPO FINANCIERO BANORTE | SERVICIOS FINANCIEROS Y DE SEGUROS | $32,006,691.00 | $36,424,892.37 |
| 2015 | COMUNICACIONES NEXTEL DE MÉXICO, S.A. DE C.V. | INFORMACIÓN EN MEDIOS MASIVOS | $4,241,780.00 | $4,462,352.00 |
| 2015 | CONCESIONARIA VUELA COMPAÑÍA DE AVIACIÓN, S.A.P.I. DE C.V. (VOLARIS) | TRANSPORTES, CORREOS Y ALMACENAMIENTO | $4,306,560.00 | $4,306,560.00 |
| 2015 | IMPULSE TELECOMMUNICATIONS DE MÉXICO, S.A. DE C.V. | INFORMACIÓN EN MEDIOS MASIVOS | $942,060.00 | $1,068,234.00 |
| 2016 | OPERADORA DE HOSPITALES ANGELES, S.A. DE C.V. | SERVICIOS DE SALUD Y DE ASISTENCIA SOCIAL | $4,601,520.00 | $4,601,520.00 |
| 2016 | STAR MÉDICA, S.A. DE C.V. | SERVICIOS DE SALUD Y DE ASISTENCIA SOCIAL | $474,760.00 | $482,926.00 |
| 2016 | BALCASA CONSULTORES, S.C. | SERVICIOS INMOBILIARIOS Y DE ALQUILER DE BIENES | $42,060.00 | $43,077.00 |
| 2018 | REPRESENTACIONES GG, S.A DE C.V. | COMERCIO AL POR MENOR | $94,362.50 | $94,362.50 |
| 2018 | TIK TEK PHARMACEUTICS, S. DE R.L. DE C.V. | COMERCIO AL POR MENOR | $15,098.00 | $15,480.00 |
| 2018 | GOT MUEBLES, S.A. DE C.V. | COMERCIO AL POR MENOR | $30,196.00 | $30,682.00 |
| 2018 | CLÍNICA DE SERVICIOS MÉDICOS COLIMAN, S.A. DE C.V. | SERVICIOS DE SALUD Y DE ASISTENCIA SOCIAL | $37,745.00 | $37,745.00 |
| | | | **$46,942,751.50** | **$51,719,498.87** |

Tabla 4.15. Multas cobradas de sanciones aplicadas por incumplimiento a los principios y demás disposiciones de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.
*Fuente: INAI, respuesta en oficio número INAI/SPDP/DGPDS/292/20.*

De igual manera adjunta una tabla en la que relaciona los montos de las sanciones emitidas por sector industrial, así como el monto correspondiente a cada sector, acumulando un monto total de $496,457,977.95, mientras que el monto total pagado solo es de $51,719,498.87, sin aportar más información que brinde certeza sobre el estatus de las sanciones que componen el resto del monto que se muestra en la siguiente tabla 4.16.

| SECTOR INDUSTRIAL: | NÚMERO MULTAS PAGADAS | IMPORTE TOTAL MULTA IMPUESTA AL SECTOR | IMPORTE MULTA PAGADA |
|---|---|---|---|
| Servicios Financieros y de Seguros | 1 | $265,988,638.10 | $36,424,892.37 |
| Servicios de Salud y de Asistencia Social | 3 | $18,032,529.16 | $5,122,191.00 |
| Transportes, Correos y Almacenamiento | 1 | $8,545,562.50 | $4,306,560.00 |
| Información en Medios Masivos | 2 | $66,459,505.10 | $5,530,586.00 |
| Industrias Manufactureras | 1 | $9,788,360.99 | $131,269.00 |
| Servicios Profesionales, Científicos y Técnicos | 1 | $13,722,143.42 | $20,399.00 |
| Comercio al Por Menor | 3 | $36,690,849.83 | $140,524.50 |

| SECTOR INDUSTRIAL: | NÚMERO MULTAS PAGADAS | IMPORTE TOTAL MULTA IMPUESTA AL SECTOR | IMPORTE MULTA PAGADA |
|---|---|---|---|
| Servicios de Esparcimiento Culturales y Deportivos, y Otros Servicios Recreativos | 0 | $17,210,059.00 | $0.00 |
| Servicios Educativos | 0 | $17,744,197.12 | $0.00 |
| Servicios de Apoyo a los Negocios y Manejo de Residuos y Desechos, y Servicios de Remediación | 0 | $19,337,840.55 | $0.00 |
| Comercio al Por Mayor | 0 | $2,955,713.18 | $0.00 |
| Servicios de Alojamiento Temporal y de Preparación de Alimentos y Bebidas | 0 | $2,733,956.00 | $0.00 |
| Servicios Inmobiliarios y de Alquiler de Bienes Muebles e Intangibles | 1 | $5,551,093.00 | $43,077.00 |
| Otros Servicios Excepto Actividades Gubernamentales | 0 | $550,879.00 | $0.00 |
| No Disponible | 0 | $384,244.00 | $0.00 |
| Agricultura, Cría y Explotación de Animales, Aprovechamiento Forestal, Pesca y Caza | 0 | $22,668.00 | $0.00 |
| Construcción | 0 | $10,135,239.00 | $0.00 |
| Corporativos | 0 | $604,500.00 | $0.00 |
| Generación, Transmisón y Distribución de Energía Eléctrica, Suministro de Agua y de Gas por Ductos al Consumidor Final | 0 | $0.00 | $0.00 |
| Minería | 0 | $0.00 | $0.00 |
| **TOTAL** | **13** | **$496,457,977.95** | **$51,719,498.87** |

Tabla 4.16. Monto de sanciones impuesta por sector vs monto de sanciones cobradas
*Fuente: INAI, respuesta en oficio número INAI/SPDP/DGPDS/292/20.*

Así entonces, queda claro que se desconoce el motivo de la diferencia entre el importe total de las multas cobradas y el importe de las multas impuestas, a interpretación, esto puede deberse a que no se ha notificado al instituto sobre la ejecución de dicha sanción, que aún se encuentra en proceso o que fueron impugnadas ante las instancias correspondientes y se resolvieron a favor de las empresas.

Lo que es preciso resaltar, es que los montos a los que se puede hacer acreedora una empresa, derivado del incumplimiento de los principios y disposiciones de la Ley, son elevados y suponen una pérdida para la empresa, puesto que, no es un gasto contemplado ni repercute positivamente, por el contrario, en el contexto de las empresas de México que, según el INEGI el 97.6% son microempresas, una sanción de esta magnitud puede poner en riesgo la continuidad del negocio.

Ante este panorama, la alternativa viable es la inversión de capital humano y económico para dar cumplimiento a la Ley, y respetar en todo momento el derecho de las personas de quienes la empresa trata datos personales, así como el desarrollo de procedimientos y mecanismos que faciliten el ejercicio de los derechos de los titulares.

*4.4. Reflexiones finales*

En cuestión normativa, existen numerables documentos legales que ayudan y orientan a los responsables a realizar el correcto tratamiento de los datos personales. Sin embargo, cuando se trata del tratamiento de datos en sistemas tecnológicos, llámese plataformas de comercio electrónico o cómputo en la nube, las leyes no alcanzan para garantizar de manera efectiva la privacidad de las personas.

De tal manera que, los responsables pueden garantizar la privacidad de las personas en cuanto a sus responsabilidades corresponda. No obstante, el uso de las tecnologías de comercio electrónico y de cómputo en la nube, incluye la intervención de tecnologías de terceros que podrían vulnerar la privacidad, contra ello, poco se puede hacer, ya que las grandes empresas tecnológicas tienen el poder para controlar el mercado, y al ser reguladas bajo la legislación de su país de residencia, dejan a la deriva a las pequeñas empresas, y más aún los derechos humanos de las personas.

Por lo anterior, es recomendable que, ante el uso de las tecnologías mencionadas, se incluya una cláusula en la que se informe a los titulares sobre las intervenciones de las tecnologías de terceros que no pueden ser controladas por el responsable, de tal manera que los titulares estén conscientes de que sus datos podrían ser recolectados y tratados por otras empresas, acto que deriva de la transacción entre el titular y el responsable.

Es notorio que se requiere avanzar hacia la alfabetización digital, lo cual supone, no solo saber implementar la tecnología de cómputo en la nube, o de comercio electrónico, sino, también dominar dichas tecnologías y conocer las implicaciones y la forma en la que intervienen terceras empresas que dominan el mercado de los datos.

Es de entender que, bajo la forma en la que operan las grandes empresas tecnológicas, la Ley de protección de datos personales de México parece obsoleta, mientras que la legislación europea ha cubierto de cierta manera las responsabilidades de dichas empresas.

No obstante, cuando se trata de implementar las medidas de seguridad, la mejor estrategia es partiendo del análisis de riesgos en base a alguna metodología, así, una vez que se conocen los riesgos, se conoce el inventario de datos y se ha determinado la brecha de seguridad, el responsable podrá implementar eficientemente las medidas de seguridad en la tecnología que le corresponde gestionar en la nube. Cuando se trata de entornos físicos, las medidas de seguridad recaen en su totalidad sobre el responsable.

Cabe destacar que las metodologías de análisis de riesgo resultan difíciles de comprender para quienes no tienen conocimientos técnicos, por tal motivo, se recomienda la integración de un equipo interdisciplinario para elaborar el análisis de riesgo, así como determinar las medidas de seguridad a implementar, pues no lo puede hacer solo un abogado ni solo un informático, sino, un equipo de trabajo que integre ambas ramas del conocimiento.

# CONCLUSIONES

La presente tesis se ha estructurado en cuatro capítulos, abordando en lo general los temas conceptuales y la naturaleza jurídica del derecho de la información, particularmente se realiza un análisis de avisos de privacidad de diez empresas que operan en México, y que sus productos y/o servicios son ofertados en línea mediante sistemas de comercio electrónico*,* concluyendo que los responsables del tratamiento de datos personales aún desconocen en su totalidad el alcance de la legislación en materia de protección de datos personales, esto hace que involuntariamente incurran en la violación del derecho a la protección de datos personales, motivo por el cual se presenta una propuesta que coadyuva a fortalecer las acciones indispensables para la armonización entre el uso de la tecnología, y el respeto a los derechos humanos.

En relación al orden de ideas que se presenta en cada capítulo, del primero se concluye que:

1. El desarrollo tecnológico ha superado por mucho el desarrollo jurídico, acontecimiento que no se puede cambiar debido a la inherente relación entre tecnología y desarrollo económico en la Sociedad de la Información.
2. La interacción entre las personas humanas y las empresas deriva en el tratamiento de grandes volúmenes de datos personales, acto que debe ser regulado por las leyes para garantizar el respeto a la privacidad de las personas.
3. El uso del cómputo en la nube en la mayoría de los casos, supone una transferencia internacional de datos por la razón de que las grandes empresas tecnológicas que ofertan este tipo de servicios, se ubican físicamente fuera del territorio mexicano, lo que deriva en la violación a este derecho al no informar a los titulares sobre dicha transferencia.
4. El potencial ilimitado de la tecnología para fines comerciales ha superado el desarrollo legislativo. Sin embargo, no se debe limitar el uso y desarrollo de la tecnología, sino, más bien, desarrollar los mecanismos que propicien el libre flujo de información y garanticen el respeto a los derechos humanos.

Por su parte, el segundo capítulo brinda un panorama general de la evolución histórica del derecho a la protección de datos personales, e identifica los sujetos del mismo con la intención de comprender que:

5. El fenómeno informativo en la Sociedad de la Información es parte intrínseca de la misma, por tanto, la Ley contempla la excepción a la comunicación de información inherente a las personas, bajo condiciones que garanticen el respeto al derecho a la protección de datos personales, limitando la recolección de los datos a los mínimos necesarios para las transacciones entre empresas y personas humanas.
6. El derecho a la protección de datos personales ha sido reconocido desde el año 1970 en Alemania, no obstante, en México se reconoce constitucionalmente hasta el año 2009. Este derecho se concibió con la intención de limitar el uso de la informática para garantizar la privacidad de las personas, ello por el potencial que estas presentan para la difusión de la información.
7. En relación al tratamiento de datos personales en entornos tecnológicos, se retoman los sujetos que identifica José María Desantes Guanter, con sus respectivas variantes acorde al derecho en cuestión y al contexto digital, identificando al sujeto universal como todos los ciudadanos que proporcionan y/o proporcionarán sus datos personales a alguna empresa; el sujeto cualificado es la persona que tiene los conocimientos jurídicos y tecnológicos necesarios para garantizar la salvaguarda de los datos, implementar medidas de seguridad y procedimientos para el ejercicio de los derechos, mientras que el sujeto organizado son todas las empresas que realizan tratamiento de datos personales.
8. Sin el conocimiento del derecho a la protección de datos personales por el sujeto universal, no se puede exigir su respeto y sin el conocimiento técnico–jurídico por parte de los sujetos organizados, no se podrá garantizar el respeto a dicho derecho.

En el capítulo tercero se realiza un análisis de los avisos de privacidad de diez empresas, con lo cual se logra probar la hipótesis, pues en la mayoría de los avisos

de privacidad no se menciona explícitamente la transferencia internacional de los datos personales. De igual manera, se observan deficiencias en lo que respecta a las facilidades que el responsable debe poner al alcance de los titulares para ejercer sus derechos, además se demuestra, como algunos protocolos de comunicación pueden poner en riesgo la privacidad de las personas, así como la falta de regulación para las empresas que operan estos protocolos, por tanto:

9. Las empresas que realizan comercio electrónico logran una ventaja competitiva, en relación a las que desarrollan su actividad comercial en el mercado tradicional, por ello, cada vez son más las empresas que se suman al comercio electrónico. Esto supone el tratamiento de datos personales en la nube, y en la mayoría de los casos también la transferencia nacional e internacional de datos, acto que no se está informando de manera adecuada en los avisos de privacidad, limitando la libertad de la autodeterminación informativa y violando el derecho a la protección de datos personales.
10. Las empresas que intervienen de manera indirecta en el comercio electrónico, como empresas de paquetería, empresas propietarias de los motores de búsqueda o servidores resolutores, también recolectan datos de los titulares, acción que en la mayoría de los casos se desconoce por el mismo responsable del tratamiento, así, el factor desconocimiento, no se cubre con la Ley y propicia la violación del derecho a la protección de datos personales.
11. En relación al punto anterior, es importante señalar que en el año 2018 México se adhirió al *Convenio 108*, ello es prueba de que la legislación en materia de protección de datos personales cumple con los requerimientos mínimos del reglamento europeo. Sin embargo, en cuanto a mecanismos de operación y acuerdos de cooperación con terceros países, aún se ve distante en comparación con la legislación europea.
12. El protocolo DNS y la nula regulación para las empresas de nombres de dominio, pone en riesgo la privacidad de los titulares al permitir que los servidores resolutores puedan generar perfiles de navegación del usuario, mismo que puede dar origen al conocimiento de información sensible.

13. El protocolo HTTP y HTTPS, aunado a la mala gestión las medidas de seguridad que la Ley obliga al responsable para su implementación, pueden propiciar el conocimiento de información que entra y sale por la red a *Internet*, comprometiendo usuarios y contraseñas de sistemas de tratamiento de datos personales, y poniendo en riesgo la confidencialidad e integridad de la información.
14. De igual manera, la intervención de terceros que ofrecen los servicios de cómputo en la nube, puede poner en riesgo la integridad y confidencialidad de la información, ante ello, el responsable poco podrá hacer, pues no tiene los permisos para gestionar la seguridad perimetral en la red de la empresa que ofrece el servicio. Aunado a que este tipo de servicios se ofertan bajo contratos de adhesión, resulta necesario que la Ley contemple responsabilidades para estas empresas, y no solo para el responsable que contrata el servicio para operar los sistemas de tratamiento de datos.

El capítulo cuarto contempla una serie de recomendaciones centradas y propuestas para a los principios, deberes y obligaciones del responsable del tratamiento de los datos, entre dichas recomendaciones se presenta la propuesta de un aviso de privacidad y un formulario para el ejercicio de derechos, los parámetros generales para la elaboración del análisis de riesgo, el inventario de datos, así como la propuesta para la implementación de medidas de seguridad administrativa y técnica, cabe precisar que:

1. Es necesario avanzar hacia la alfabetización digital empresarial, de tal manera que el uso de las tecnologías cubra todos los vectores de riesgo para la privacidad, sin minar el beneficio que ofrecen para el desarrollo económico, en tal sentido, las tecnologías que se desarrollen deberán tener un enfoque de privacidad por defecto y por diseño.
2. La elaboración del documento de seguridad de datos personales, es indispensable para gestionar de manera eficiente los riesgos inherentes a los datos, pues de este documento derivan las medidas de seguridad administrativas, técnicas y físicas a las que se refiere el artículo 19 de la Ley.

3. Si bien el departamento de datos personales debe contar con una persona conocedora de derecho y tecnología, que garantice el cumplimiento de la Ley y coadyuve en el desarrollo del documento de seguridad; las acciones para la gestión y mitigación de los riesgos detectados, se deben elaborar por un equipo de trabajo interdisciplinario, no solo por un abogado, un tecnólogo o por el responsable de datos personales, pues cada quien puede aportar valor desde su área de conocimiento, y aplicar de manera eficiente los recursos necesarios para garantizar la integridad y confidencialidad de la información. Por ello se recomienda la intervención de personas con conocimientos de derecho, tecnología y normalización.

FUENTES DE INVESTIGACIÓN

## Bibliográficas

Agencia Española de Protección de Datos, *Esquema de certificación de delegados de protección de datos de la agencia española de protección de datos (esquema aepd-dpd),* 2019, https://www.aepd.es/sites/default/files/2020-07/esquema-aepd-dpd.pdf.

Agencia española de Protección de Datos. *Privacidad en DNS*. 2019. p. 2. https://www.aepd.es/sites/default/files/2019-12/nota-tecnica-privacidad-dns.pdf

AGUILERA GARCÍA, Edgar Ramón, *Inteligencia Artificial Aplicada al Derecho,* México, Universidad Nacional Autónoma de México, 2007.

AGUIRRE NIETO, Marisa, “El Derecho de la Información como Ciencia”, en BEL MALLEN, Ignacio y CORREDOIRA Y ALFONSO, Loreto, (ccord.), *Derecho de la Información,* España, Editorial Ariel, S.A., 2003.

ARENAS RAMIRO, Mónica, "El Reconocimiento de un Nuevo Derecho en el Ordenamiento Jurídico Español: El Derecho Fundamental a la Protección de Datos Personales", en PÉREZ PINTOR, Héctor (coord.), *El Iusinformativismo en España y México,* Morelia, Michoacán, México: División de Estudios de Posgrado de la Facultad de Derecho y Ciencias Sociales UMSNH, 2009.

ARIAS, Ángel, *Computación en la Nube, 2a. ed.,* s.l.i., 205.

AUREN IBEROAMERICA, *Estudio de Cultura sobre Tratamiento de Datos Personales en el Sector de las Tecnologías de la Información,* CANIETI, Secretaría de Economía y PROSOFT 2.0, s.f.

BÁRDAN ESQUIVEL, Cuitláhuac y RIVERA PAZ, Gustavo (coords.), *Micro, Pequeñas y Medianas Empresas en México. Evolución, Funcionamiento y Problemática*, México, Instituto de Investigaciones Legislativas del Senado de la República, 2002, p. 12.

BEAVER, Kevin, *Tips and Tricks Guide To Software Security Assurance,* https://www.principlelogic.com/docs/Tips_and_Tricks_Guide_to_Software_Security_Assurance.pdf.

CARR, Nicholas, *Superficiales,* Taurus, México, D.F., 2015.

CAVOUKIAN, Ann, *Privacy by Design,* 2006, https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

CEPAL, *La cumbre del milenio,* 2000, https://www.cepal.org/es/temas/objetivos-de-desarrollo-del-milenio-odm/acerca-odm.

Cfr. Agencia Española de Protección de Datos, *Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos (Esquema AEPD-DPD),* 13 de junio 2018, https://www.aepd.es/reglamento/cumplimiento/common/esquema-aepd-dpd.pdf

*Cfr.* Agencia Española de Protección de Datos, *Estándares Internacionales sobre Protección de Datos Personales y Privacidad.* Resolución de Madrid, 2009, pp. https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf.

CHIAVENATO, Idalberto, *Iniciación a la Organización y Técnica Comercial,* México, Mc Graw Hill, 1993.

CHIAVENATO, Idalberto, *Introducción a la Teoría General de la Administración, 7a ed.*, México, McGraw-Hill Interamericana, 2006.

DAVARA FERNÁNDEZ DE MARCOS, Isabel, *El derecho al olvido en relación con el derecho a la protección de datos personales,* Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, 2014, http://www.infodf.org.mx/capacitacion/publicacionesDCCT/ensayo23/23ensayo2014.pdf

DESANTES, José María, *Derecho a la información. Materiales para un sistema de la comunicación*, Fundación COSO, España, 2004.

DESANTES, José María, *Fundamentos del Derecho de la Información,* Confederación Española de Cajas de Ahorros, Madrid, 1977.

GARCÍA HERNÁNDEZ, Sonia, “Inteligencia de Negocios para Incrementar la Competitividad en MiPYMES”, en ARREOLA TALAVERA, Alma Yunuen y PALOMARES VAUGHAN, Luis Antonio (coords.), *Competitividad Global a Través del Emprendimiento e Innovación,* Morelia, CONLAMI, Universidad Michoacana de San Nicolás de Hidalgo, 2018, pp. 624-645.

GARCÍA TINAJERO, Leonel, El Monopolio Mediático en México: toque de queda al derecho a la información", en PONCE BÁEZ, Gabriela y GARCÍA TINAJERO, Leonel (coor.), *Las Fronteras del derecho de la información,* México, Novum, 2011.

GONZÁLEZ DÍAZ, Isaac, *Big Data para CEO's y Directivos de Marketing,* Kindle, versión electrónica, 2017.

GONZÁLEZ, Agustín, *Computación en la Nube,* Universidad Técnica Federico Santa María, 2009.

GUZMÁN GARCÍA, María de los Ángeles, *El derecho fundamental a la protección de datos personales en México: Análisis desde la influencia del ordenamiento jurídico español,* Universidad Complutense de Madrid, 2013, p. 60, https://eprints.ucm.es/22817/1/T34727.pdf.

HERNÁNDEZ Y RODRÍGUEZ, Sergio, *Introducción a la Administración,* México, McGRAW-HILL, 2011.

INAI, *Conceptos General de la Protección de Datos Personales,* 2019, https://www.cinvestav.mx/ Portals/0/sitedocs/tyr/GuiaTitulares-01_PDF.pdf.

INAI, *Expediente PPD.02.13/16,* 2016, http://inicio.ifai.org.mx/pdf/resoluciones/2016/PPD%200213.pdf

INAI, *Guía de Esquemas de Autorregulación en Materia de Protección de Datos Personales,* 2016, http://cevifaiprivada.ifai.org.mx/pluginfile.php/14423/mod_data/content/15/Gu%C3%ADa%20de%20Esquemas%20de%20Autorregulaci%C3%B3n%20en%20Materia%20de%20Protecci%C3%B3n%20de%20Datos%20Personales.pdf.

INAI, *Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* México, 2016, p. 69, http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_junio2016.pdf

INAI, *Guía para el Tratamiento de Datos Biométricos,* 2018, http://inicio.ifai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf.

INAI, *Guía para instrumentar medidas compensatorias,* 2016, http://inicio.ifai.org.mx/ DocumentosdeInteres/Guia_para_instrumentar_medidas_compensatorias.pdf.

INAI, *Los Derechos ARCO,* 2019, https://www.cinvestav.mx/ Portals/0/sitedocs/tyr/ GuiaTitulares-03_PDF.pdf.

INAI, *Metodología de Análisis de Riesgos BAA,* 2015, http://inicio.ifai.org.mx/ DocumentosdeInteres/Metodolog%C3%ADa_de_An%C3%A1lisis_de_Riesgo_ BAA(Junio2015).pdf.

INAI, *Principios Rectores de la Protección de Datos Personales,* 2019, https://www.cinvestav.mx/ Portals/0/sitedocs/tyr/GuiaTitulares-02_PDF.pdf.

INAI, *Principios y deberes en materia de Protección de Datos Personales,* México, Espacio de Formación Multimodal, p. 65.

INAI, *Procedimientos de datos personales ante el INAI,* 2019, https://www.cinvestav.mx/ Portals/0/sitedocs/tyr/GuiaTitulares-04_PDF.pdf.

INAI. *Guía para Titulares de los datos personales, Volumen 4: Procedimientos de datos personales ante el INAI.* http://inicio.inai.org.mx/Guias/Guia%20Titulares-04_PDF.pdf

INCIBE. *Estudio del Estado de DNSSEC en España.* 2018. https://www.incibe-cert.es/sites/default/files/contenidos/estudios/doc/incibe_estudio_del_estado_de_dnssec_en_espana_0.pdf.

Instituto Nacional de Estadística y Geografía, *Boletín de Prensa Núm. 285/16*, Aguascalientes, 2016.

Instituto Nacional de Estadística y Geografía, *Clasificación de las Actividades Económicas,* s.f., http://www3.inegi.org.mx/rnm/index.php/ catalog/205/download/5998.

JIMÉNEZ ROSANO, Martha Cristina, *El ensayo fotográfico como Diseño de Información. El uso de la fotografía en la investigación exploratoria de un fenómeno social*, Puebla, Universidad de las Américas Puebla, 2005, http://catarina.udlap.mx/u_dl_a/tales/documentos/ldf/jimenez_r_mc/.

JOYANES AGUILAR, Luis, *Computación en la Nube,* Ciudad de México, Alfaomega, 2012.

KENNETH C., Laudon y GUERCIO TRAVER, Carol, *E-commerce 2013. Negocios, Tecnologías y Sociedad,* Pearson Educación, México, 2014.

LANIER, J. *Diez razones para borrar tus redes sociales de inmediato,* Barcelona, España, 2018.

LIPNER, Steve, "The trustworthy computing security development lifecycle", *ResearchGate,* 2005, https://www.researchgate.net/publication/4115440_The_trustworthy_computing_security_development_lifecycle.

MENDES, Jorge, *Big Data La primera guía completamente en español explica Big Data y sus aplicaciones,* Kindle, versión electrónica, 2018.

Microsoft, *Writing Secure Code,* 2003, https://ptgmedia.pearsoncmg.com/images/978073561722 3/samplepages/9780735617223.pdf

National Institute of Standards and Technology, *NIST Cloud Computing Standards Roadmap, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-291r2.pdf*

PEIRANO, Martha, *El enemigo conoce el sistema,* Penguin Random House Grupo Editorial, Barcelona, 2019.

PRIMORAC, Carlos R., *Computación en Nube,* Universidad Nacional del Nordeste, 2014.

Red Iberoamericana de Protección de Datos, *Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana,* 2007, http://www.redipd.es/actividades/encuentros/ V/common/9_nov/Directrices_de_armonizacion.pdf.

RIVERA SANCLEMENTE, María del Rosario, *La evolución de las estrategias De marketing en el entorno Digital: implicaciones jurídicas,* [Tesis doctoral], Universidad Carlos III, Madrid, 2015, https://e-archivo.uc3m.es/bitstream/handle/10016/22498/rosario_rivera_tesis.pdf.

ROMERO MONSERRAT, George Alexis, *Solución de Marketing Interactivo de Proximidad Basado en Tecnologías de Campo Cercano,* Universidad de Cantabria, 3014, https://pdfs.semanticscholar.org/023e/8565e73a3b6362a45b14aaee361d8f825cdb.pdf.

Secure Sofware, Inc., *The CLASP Application Security Process,* 2005, https://cwe.mitre.org/documents/sources/TheCLASPApplicationSecurityProcess.pdf.

STIGLITZ, Joseph Eugene y Greenwald, Bruce Corman Norbert, *La creación de una sociedad del aprendizáje,* Ediciones Cultrales Paidós, México D.F., 2014

TURNER, Colin, *E-conomía de la información*, España, Ediciones Deusto, S.A., 2001.

UNESCO, *La UNESCO y la sociedad de la información para todos,* 1996, https://unesdoc.unesco. org/ark:/48223/pf0000108540_spa.

VILLANUEVA, Ernesto y DÍAZ, Vanessa, *Derecho de las Nuevas Tecnologías,* México: Oxford University Press México, 2015.

VILLANUEVA, Ernesto, *Derecho de la Información,* México, Miguel Ángel Porrúa, 2006.

WP, *Directrices sobre los delegados de protección de datos (DPD),* 13 de diciembre de 2016, https://www.aepd.es/media/criterios/wp243rev01-es.pdf.

## Hemerográficas

ALFONSO SÁNCHEZ, Ileana R., "La Sociedad de la Información, Sociedad del Conocimiento y Sociedad del Aprendizaje. Referentes en torno a su formación", *Reflexiones,* Núm. 2, Vol. 12, 2016, https://dialnet.unirioja.es /descarga/articulo/5766698.pdf.

AVALOS ROSADO, Marco Carlos, *La sociedad del conocimiento,* San Luis Potosí, México, 2013, https://static1.squarespace.com/static/51ede959e4b0de4b8d24e8a9/t/5213aa19e4b0750ce7ecb4c6/1377020441113/1.+La+sociedad+del+conocimiento.pdf

AVELEYRA, Antonio M. 2003. "El Derecho de Acceso a la *Información Pública vs. el Derecho de Libertad Informática". Jurídica-Anuario, Revista de la Universidad Iberoamericana (32):* 403–443. https://revistas-colaboracion.juridicas.unam.mx/index.php/juridica/article/download/11488/10520.

COMISIÓN EUROPEA, *Antimonopolio: La Comisión impone a Google una multa de cerca de 4,34 miles de millones EUR por prácticas ilegales en relación con los dispositivos móviles Android para reforzar la posición dominante del motor de*

*búsqueda de Google,* 2018, [en línea], https://ec.europa.eu/commission/presscorner/detail/es/IP_18_4581.

GARCÍA MARCO, Francisco Javier, “El Concepto de Información: Una aproximación transdisciplinar”, *Revista General de Información y Documentación,* Vol. 8, Núm. 1., Madrid, Servicio de Publicaciones Universidad Complutense, 1998.

GARRIGA DOMÍNGUEZ, Ana, “El derecho a la protección de datos personales en la jurisprudencia del tribunal constitucional”, *Nuevos retos para la protección de Datos Personales. En la Era del Big Data y de la computación ubicua,* Dykinson, 2015.

HERNANGÓMEZ BARAHONA, Juan José, "La empresa como organización: una propuesta de delimitación de su concepto", *Anales de estudios económicos y empresariales,* núm. 3, pp. 225- 238, 1988, https://dialnet.unirioja.es/servlet/articulo?codigo=785516.

LÓPEZ AYLLÓN, Sergio, "Democracia y Acceso a la Información", *Colección de cuadernos de Divulgación sobre Aspectos doctrinarios de la Justicia electoral, No. 9*, Edit. Tribunal Electoral del Poder Judicial de la Federación, México, 2005.

OTTER, Thomas y Mónica Cortez, *Economía de la Información, Sociedad de la Información, Información Periodística: Elementos compartidos hacia una información pluralista y equitativa,* Konrad-Adenauer-Stiftung, Lima, 2003, https://paisdospuntocero.files.wordpress.com/2015/04/18-kas_4901-1522-4-303.pdf.

PÉREZ GIL, Julio, “El Nuevo Papel De La Telefonía Móvil En El Proceso Penal: Ubicación y Perfiles De Desplazamiento.” *El Proceso Penal En La Sociedad De La Información. Las Nuevas Tecnologías Para Investigar y Probar El Delito,* Universidad de Burgos, 2012, https://www.academia.edu/33767738/El_nuevo_papel_de_la_telefon%C3%ADa_m%C3%B3vil_en_el_proceso_penal_ubicaci%C3%B3n_y_perfiles_de_desplazamiento?source=swp_share.

PFEFFER URQUIAGA, Emilio, "Los derechos a la intimidad o privacidad, a La honra y a la propia imagen. Su protección frente a la libertad de opinión e información", *Ius et Praxis,* núm. 1m vol. 6, 2000, http://www.redalyc.org/pdf/197/19760123.pdf.

PowerData, *Del bit… al Big Data,* s.a., *http://cdn2.hubspot.net/hub/239039/file-359994269-pdf/docs/PowerData_-_Del_bit%E2%80%A6_Al_Big_Data.pdf.*

RIOS ORTEGA, Jaime, "El concepto de información: dimensiones bibliotecológica, sociológica y cognoscitiva", *Investigación Bibliotecológica,* Vol. 28, Núm. 62, enero/abril 2014.

RUÍZ GARCÍA, Jesús; Baño Gimeno, M.A. Pilar y Secadas Marcos, Francisco, "Evolución Histórica de la Escritura" *Estudios*, Madrid, España, 1985.

SÁNCHEZ, Carlos y Humberto Rios, "La economía del conocimiento como base del crecimiento económico en México", *Enl@ce: Revista Venezolana de Información, Tecnología y Conocimiento,* Núm. 2, Vol. 8, 2011, pp. 43-60, https://www.redalyc.org/pdf/823/82319126004.pdf

SEVILLANO PÉREZ, Felipe, "Big Data", *Economía industrial, (Ejemplar dedicado a: Ciudades inteligentes),* núm. 395, 2015, pp. 71-86, https://www.mincotur.gob.es/Publicaciones/Publicaciones periodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/395/F%20SEVILLANO%20PEREZ.pdf.

VILASAU SOLANA, Mónica, "El caso Google Spain: la afirmación del buscador como responsable del tratamiento y el reconocimiento del derecho al olvido (análisis de la STJUE de 13 de mayo de 2014)", *Revista de los Estudios de Derecho y Ciencia Política,* Núm. 18, Junio 2014, pp. 16 - 32, http://openaccess.uoc.edu/webapps/o2/bitstream/10609/93657/1/CasoGoogleSpain.pdf

## Legislación

Diario Oficial de la Federación, *Ley para el Desarrollo de la Competitividad de las Micro, Pequeña y Mediana Empresa,* Reforma publicada en el DOF el 19-05-2017, http://www.diputados.gob.mx/LeyesBiblio/pdf/247_190517.pdf.

Diario Oficial de la Federación, *ACUERDO por el que se establece la estratificación de las micro, pequeñas y medianas empresas,* Secretaría de Economía, 2009.

Diario Oficial de la Federación, *Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* Publicada en el DOF el 5-julio-2010, http://www.diputados.gob.mx/LeyesBiblio/ pdf/LFPDPPP.pdf

ONU, *Declaración Universal de Derechos Humanos,* Adoptada y proclamada por la Asamblea General en su resolución 217 A (III), de 10 de diciembre de 1948, https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf.

ONU, *Pacto Internacional de Derechos Civiles y Políticos,* Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966. https://www.ohchr.org/SP/Professional Interest/Pages/CCPR.aspx

Diario Oficial de la Federación, *Constitución Política de los Estados Unidos Mexicanos,* http://pdba.georgetown.edu/Constitutions/Mexico/Mexico2009.pdf

Diario Oficial de la Unión Europea, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo,* 27 de abril de 2016, art. 39, https://www.boe.es/doue/ 2016/119/L00001-00088.pdf.

Internal Revenue Service, *Privacy Act of 1974,* https://www.federalregister.gov/ documents/2018/06/11/2018-12462/privacy-act-of-1974

Diario Oficial de la Federación, *Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* publicado el 21 de diciembre de 2011.

OCDE, *Directrices de la OCDE que regulan la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales,* Ministerio de Administraciones Públicas, http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf.

Diario Oficial de la Federación, *Ley Federal de Telecomunicaciones y Radiodifusión,* reformada 15-06-2018, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR_ 020419.pdf.

OCDE, *Recomendación del Consejo de la OCDE relativo a los Lineamientos para la Protección al Consumidor en el Contexto del Comercio Electrónico,* OCDE, 1999, https://www.oecd.org/sti/consumer/34023784.pdf.

OCDE, *Declaración Ministerial relativa a la Protección de la Intimidad en las redes Globales,* OCDE, 1998, http://www.oas.org/es/sla/ddi/docs/Declaracion_OCDE_Proteccion_Intimidad_redes.pdf.

Diario Oficial de la Federación, *Ley Federal de Protección al Consumidor,* Reformada DOF, 12-04-2019, http://www.diputados.gob.mx/LeyesBiblio/pdf/113_120419.pdf.

Diario Oficial de la Federación, *Código de Comercio,* Reformado DOF, 28-03-2018, http://www.diputados.gob.mx/LeyesBiblio/pdf/3_301219.pdf

Diario Oficial de la Unión Europea, *Versión consolidada del tratado de funcionamiento de la unión europea,* 2012, https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12012E/TXT &from=ES.

Diario Oficial de las Comunidades Europeas, *Carta de los derechos fundamentales de la unión europea,* 2000, https://www.europarl.europa.eu/charter/pdf/text_es.pdf.

Consejo de Europa, *Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal,* 1981, https://rm.coe.int/16806c1abd.

Organización de las Naciones Unidas, *Principios Rectores para la Reglamentación de los Ficheros Computadorizados de Datos Personales,* http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2015.pdf.

Diario Oficial, *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 estos datos*, https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=EN.

APEC, *Marco de Privacidad,* http://www.apecsec.org.sg/apec/news__media/fact_sheets/about_apec.html.

Diario Oficial de la Federación, *Lineamientos del Aviso de Privacidad,* Secretaría de Economía, 2013, http://www.dof.gob.mx/nota_detalle.php?codigo=5284966&fecha=17/01/2013.

Diario Oficial de la Federación, *Parámetros de Autorregulación en Materia de Protección de Datos Personales,* Secretaría de Economía, 2014, https://www.economia.gob.mx/files/marco_normativo/ PAR1.pdf.

## Cibergráficas

BAUTISTA BAUTISTA, Gerardo, *Clasificación de las empresas en México*, Universidad Autónoma del Estado de Hidalgo, https://www.uaeh.edu.mx/scige/boletin/prepa4/n5/m14.html

CENDEJAS JÁUREGUI, Mariana, *Manual de Autoformación sobre la Ley de Protección de Datos Personales para el Distrito Federal,* México: Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, 2009.

Cenépolis, *Cinema Park,* [en línea], https://fundacioncinepolis.org/programa-cinema-park.php.

Cenépolis, *Sla de Arte Cinépolis,* [en línea], https://cinepolis.com/sala-de-arte.

Ciépolis, *¿Qués es CineCash Cinépolis?,* [en línea]. https://cinepolis.com/HTML/ Otros/landing-cinecash/cinecash.html.

Cinepremiere, *Cinépolis VR ofrecerá experiencias de videojuegos de realidad virtual,* [en línea], 2017, https://www.cinepremiere.com.mx/cinepolis-vr-experiencias-realidad-virtual.html.

CONDUSEF, *Comercio Electrónico, la ompra y venta de bienes y servicios a través de internet,* [en línea], https://www.condusef.gob.mx/gbmx/?p=comercio-electronico.

E-commerce Award, E*stas son las empresas finalistas ecommerce award mexico 2018,* [en línea], https://ecommerceaward.org/estas-son-las-empresas-finalistas-ecommerce-award-mexico-2018/

Grupo Elektra, *Acerca de Grupo Elektra,* [en línea], http://www.grupoelektra. com.mx/es/sustentabilidad/quienes-somos.html.

IETF. *DNS Privacy Considerations.* 2015. https://www.rfc-editor.org/rfc/rfc7626.txt

IETF. *DNS Queries over HTTPS (DoH).* 2018. https://tools.ietf.org/html/rfc8484.

IETF. *Domain Names - Concepts and Facilities.* 1987. https://www.ietf.org/rfc/rfc1034.txt

IETF. *Domain Names - Implementation and Specification.* 1987. https://www.ietf.org/rfc/rfc1035.txt

IETF. *Specification for DNS over Transport Layer Security (TLS).* 2016. https://tools.ietf.org/html/rfc7858.

INAI, *¿En qué consiste el derecho de protección de datos personales?,* http://inicio.ifai.org.mx/SitePages/Como-ejercer-tu-derecho-a-proteccion-de-datos.aspx?a=m1

Interjet, *Quienes somos,* [en línea], https://www.interjet.com/es-mx/experiencia-interjet/viajando-con-interjet/quienes-somos.

Peixe, *Acerca de Peixe,* [en línea], https://www.groupon.com.mx/e/acerca-de.

Price Travel, *Acerca de PriceTravel,* [en línea], https://www.pricetravel.com.mx/info/acerca-nosotros.

PROFECO, *Monitoreo de Tiendas Virtuales,* 2019, [en línea], https://www.gob.mx/profeco/documentos/monitoreo-de-tiendas-virtuales-114564?state=published.

Real Academia de la Lengua Española, *Información,* [En línea], 2019, http://dle.rae.es/ ?id=LXrOqrN.

Root-servers.org. https://root-servers.org/.

TopReviews, *Comparativa antivirus 2020.* 2020, https://www.topreviews.eu/es/mejor-antivirus/.

# ANEXO 1

## CONTROL DE ACCESO A LOS SISTEMAS DE TRATAMIENTO DE DATOS PERSONALES

### OBJETIVO

Establecer los parámetros para mantener actualizado el control de usuarios que acceden a los sistemas de tratamiento de datos personales.

### ACTUALIZACIÓN

Este control deberá actualizarse cada que se dé de baja un usuario, se agreguen o se eliminen, con la intención garantizar la integridad y confidencialidad de los datos.

### INVENTARIO DE USUARIOS Y ACCESO A LOS SISTEMAS

| No | Nombre | Usuario | Sistema | Permisos | Alta | Baja |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| 2 | | | | | | |
| 3 | | | | | | |
| 4 | | | | | | |
| 5 | | | | | | |
| 6 | | | | | | |
| 7 | | | | | | |
| N | | | | | | |

Fecha de actualización

# POLÍTICA PARA LA GESTIÓN DE USUARIOS

## OBJETIVO

Establecer el procedimiento para altas y bajas de usuarios de acceso a los sistemas de tratamiento de datos personales.

## RESPONSABLE DEL PROCEDIMIENTO

Se designa como responsable del procedimiento al jefe del Departamento de Sistemas, quien tendrá la obligación de dar respuesta a las solicitudes de alta y bajas de los usuarios cuando así le sea solicitado, así como de mantener actualizado el control de usuarios.

## PROCEDIMIENTO PARA ALTA DE USUARIOS

Cuando alguna área requiera acceso al sistema para el cumplimiento de sus funciones laborales, deberá realizar la solicitud por escrito y con firma de su superior inmediato al Departamento de Sistemas, especificando el sistema al cual requiere acceder, las actividades a realizar, así como el cargo del usuario dentro de la empresa.

El jefe de sistemas, en un plazo no mayor a 24 horas hábiles, dará respuesta por escrito, entregando el usuario y la contraseña a la persona solicitante, asimismo, procederá a registrar los datos correspondientes en el control de usuarios.

## PROCEDIMIENTO PARA BAJA DE USUARIOS

Cada responsable de área está obligado a notificar al Departamento de Sistemas sobre la separación laboral de los empleados, mientras que el jefe de sistemas es el responsable de dar de baja los usuarios en los sistemas, así como de actualizar el control de usuarios.

## RESPONSABILIDADES DEL USUARIO

El usuario de los sistemas de tratamiento de datos personales, tiene la responsabilidad de hacer buen uso de sus claves de acceso, de cuidar y

mantenerlas confidenciales ante terceros no autorizados, aun cuando se trate de compañeros de la misma empresa.

Es recomendable que dichos datos no se escriban en papel, se peguen en el monitor de la computadora, se configuren para que los navegadores los recuerden o se envíen por correo electrónico. En su caso, podrá hacer uso de una bóveda de contraseñas en la computadora que le haya sido designada para el desempeño de sus actividades, misma que deberá tener contraseña de inicio de sesión.

La vulneración por descuido o negligencia será motivo de procedimientos administrativos, según lo estime la dirección de la empresa y acorde a los daños ocasionados, tanto para la empresa como para los clientes de la misma.

### CAMBIOS DE CONTRASEÑA

Con la intención de evitar vulnerabilidades a los sistemas de tratamiento de datos personales, es necesario que el usuario cambie su contraseña cada tres meses, por ello, cuando se cumpla este periodo, el sistema solicitará el cambio de contraseña, previa autenticación con la contraseña actual, la contraseña nueva deberá contener mínimo 12 caracteres, entre los que debe contener letras mayúsculas, números y caracteres especiales como asteriscos, guiones, comas o similar.

### RESPONSABILIDAD DE INFORMACIÓN

Si el usuario sospecha que su clave de acceso ha sido comprometida, debe notificarlo de inmediato al Departamento de Sistemas para que se proceda a bloquear dicho usuario y generar uno nuevo para la continuidad de las actividades laborales.

Lugar y fecha de entrada en vigor

# ANEXO 2

## POLÍTICAS PARA EL USO DEL CORREO ELECTRÓNICO INSTITUCIONAL

TIPO DE DOCUMENTO: POLÍTICA

CLASIFICACIÓN: BUENAS PRÁCTICAS

### INTRODUCCIÓN

La “empresa”, proporciona a todos los empleados que así lo requieran, una cuenta de correo electrónico. El usuario final de dicha cuenta será el responsable del buen uso y de los contenidos que mediante este correo se transfieran.

Por tanto, el Departamento de Sistemas a través de la experiencia en el uso de sistemas y servicios tecnológicos, ha identificado áreas de mejora que coadyuvan al adecuado uso del correo electrónico y garantizan la continuidad de las comunicaciones establecidas entre las áreas y actores externos que solicitan o proporcionan algún servicio y/o producto a la institución.

De ahí que se considere necesaria la adecuada instrumentación, gestión y empleo de las tecnologías de la información y comunicación con la finalidad de que las personas que laboran en esta empresa, conozcan los lineamientos para el uso adecuado de esta tecnología, como una herramienta de comunicación necesaria para el desempeño de sus funciones.

En relación a lo anterior, este documento tiene por objeto:

- **a)** Establecer los lineamientos de utilización del correo electrónico por los usuarios, con el fin de garantizar su uso correcto.
- **b)** Informar de las obligaciones que asumen los usuarios como consecuencia de dicho uso.
- **c)** Informar de la existencia de controles por parte de la empresa con la intervención mínima necesaria y solo para aquellos casos especificados.

### Objetivo

Establecer los lineamientos para el uso adecuado del correo electrónico institucional, con la finalidad de evitar incidentes de seguridad y garantizar la continuidad de las comunicaciones establecidas con actores externos, bajo los principios de transparencia y protección de datos personales.

### Alcance

Normar el uso, aprovechamiento y administración del correo electrónico que la “empresa” proporciona a los empleados como medio de comunicación oficial para el desempeño de sus funciones.

Los presentes lineamientos aplican para todos los usuarios que usan una cuenta de correo electrónico institucional, y tiene como finalidad generar una cultura de responsabilidad ante el uso del correo electrónico, el cual, al igual que el contenido que en él se maneja, es propiedad de la empresa.

### Vigencia

Este documento entra en vigor a partir de su autorización y su vigencia es por tiempo indefinido, debiendo adecuarse a los cambios y a las necesidades de la empresa y a las tecnologías emergentes.

## Disposiciones Generales

### Concepto de Correo Electrónico

El correo electrónico es un sistema de mensajería que facilita la transmisión de mensajes sin limitación de fronteras, permitiendo la comunicación entre personas sin que se encuentren conectados a través de un medio físico. Este servicio puede ser proporcionado por un servidor de correo público o privado; en ambos casos, dichos servidores requieren de conexión a *Internet* para poder operar.

Los servidores de correo electrónico, almacenan de manera temporal los contenidos para que estén disponibles para emisores y receptores, por lo que la información que se transfiera mediante este servicio, quedará almacenada en manos de un tercero, desde donde será accedida por las partes intervinientes en la comunicación.

### La Dirección de Correo Electrónico

La dirección de correo electrónico que se les entrega a los empleados de la empresa, son administradas por un servidor de correo privado, “empresa que presta el servicio de correo electrónico”, al cual se acede mediante el dominio “especificar dominio”.

En caso de ser necesario, este correo podrá ser proporcionado por un servidor de correo electrónico en una nube pública como es Gmail.com u Outlook.com, o cualquier otro servidor sin distinción de su localización geográfica. En todo caso, dicho correo deberá ser proporcionado por la empresa para fines laborales, y se agregará al resguardo de los bienes tangibles e intangibles asignados al usuario para el desempeño de sus funciones.

### *De la Transferencia de Información Personal*

El correo, al ser un servicio proporcionado por un tercero externo a la empresa, es importante tomar en cuenta que el manejo de datos personales es un tema delicado, ya que al usarse este servicio para el envío y recepción de información en la que se incluyan datos personales, se debe corroborar que exista el consentimiento del titular de dichos datos personales, pues al usar la tecnología de nube, siempre se almacenará una copia del contenido de los correos electrónicos en los servidores del tercero que proporciona el servicio del correo electrónico.

Por lo anterior, es necesario cuidar que el aviso de privacidad contemple dicho tratamiento de los datos personales, con la intensión de que el titular tenga la facultad para controlar quien, donde, como y para que almacenan sus datos personales.

### *De la Propiedad del Correo Electrónico y su Contenido*

La empresa es la propietaria de toda la información que se envía y recibe mediante el correo electrónico institucional. Por tal motivo, el usuario deberá evitar hacer uso del correo electrónico institucional para comunicaciones de índole personal.

El gerente o la persona que el designe por escrito, podrá auditar los contenidos de los correos en caso de que exista sospecha de mal uso de la información a través

de medios electrónicos, por necesidades del servicio o cuando el propietario no se encuentre presente y se requiera información del correo electrónico que se le haya asignado.

La contraseña del correo se le proporciona a cada uno de los resguardantes, y en caso que decidan cambiar dicha contraseña, deberán notificarlo al Departamento de Sistemas, con la finalidad de mantener actualizada la lista de las contraseñas de correos electrónicos institucionales y no afectar la operabilidad de la empresa.

*DEL USO DEL CORREO ELECTRÓNICO*

El uso del correo electrónico deberá ser estrictamente para tratar asuntos relacionados con las funciones laborales encomendadas. Queda estrictamente prohibido el uso de dicho correo para tratar temas personales o de cualquier otra índole que no se relacione directamente con las funciones encomendadas.

*DE LA RESPONSABILIDAD DEL USUARIO*

Cada usuario es responsable del manejo de la información y del contenido que comunican a través del correo electrónico institucional, por lo que estarán sujetos a las responsabilidades derivadas por omisiones o acciones negligentes, dolosas y/o de mala fe, para las que hagan uso del correo electrónico institucional.

Los usuarios deberán velar por mantener una adecuada comunicación bajo los principios éticos, morales, de confidencialidad y privacidad, ya que el uso negligente puede derivar en amonestaciones o en sanciones administrativas.

*DE LA SEGURIDAD DE LA INFORMACIÓN*

Por tratarse de un servicio proporcionado por un tercero, el personal de informática de la empresa no tiene el control de los equipos en los cuales se almacena la información; el Departamento de Sistemas se deslinda de toda responsabilidad, por lo que el usuario resguardante será el responsable de mantener las copias de seguridad en su computadora, para garantizar que dicha información esté disponible en el momento que la requiera.

En cuanto a la privacidad de la información, se especula que el prestador del servicio ha implementado medidas de seguridad administrativas, técnicas y físicas

para garantizar la privacidad de la información y mantenerla fuera del conocimiento de personas ajenas a su tratamiento.

De manera enunciativa más no limitativa, los usuarios deberán cumplir con las siguientes medidas de seguridad:

a) Guardar el usuario y la contraseña de acceso a la cuenta de correo de forma segura y no facilitarlos a otras personas, a excepción del personal de sistemas para efectos de control y para las disposiciones señaladas con anterioridad.
b) No utilizar una contraseña fácilmente deducible.
c) No hacer uso de la opción que se le ofrece al usuario para guardar la contraseña en el navegador web para evitar reintroducirla en cada conexión. Esta debe ser escrita en cada conexión por seguridad.
d) Desconectarse del correo electrónico y bloquear el equipo de cómputo, en caso de ausentarse de su lugar de trabajo.
e) No seguir cadenas de mensajes piramidales.
f) No abrir mensajes sospechosos que puedan provocar daños a la información del usuario o a la institución en general.
g) No enviar, reenviar o responder a mensajes de correo que contengan datos sensibles, sin la autorización del responsable de los datos personales.
h) En caso de detectar una incidencia durante el uso del correo electrónico, el usuario debe ponerlo en conocimiento del personal de informática de la empresa.

*CESE DE LA RELACIÓN LABORAL*

Sabidos de que el correo asignado es propiedad de la empresa, el usuario está obligado, además de cuidar y hacer buen uso del mismo, a incluir dicho correo y contraseña en el acta de entrega-recepción del área correspondiente cuando así se le requiera, para que la persona que va a cubrir las funciones laborales pueda continuar utilizando dicho correo para la consecución de las actividades del área.

Lugar y fecha

# ANEXO 3

## POLÍTICAS PARA EL USO DE EQUIPO DE CÓMPUTO

TIPO DE DOCUMENTO: POLÍTICA

CLASIFICACIÓN: BUENAS PRÁCTICAS

### INTRODUCCIÓN

La “empresa”, proporciona a sus empleados que así lo requieran, un equipo de cómputo para el desempeño de las funciones encomendadas, el cual, el usuario tiene la responsabilidad de aprovechar y cuidar de manera ética y profesional, consciente que el uso negligente del mismo puede ocasionar perdidas para la empresa y acciones administrativas hacia su persona.

En relación a lo anterior, este documento tiene por objeto:

- **a)** Establecer los lineamientos de utilización del equipo de cómputo por los usuarios, con el fin de garantizar su uso correcto.
- **b)** Informar de las obligaciones que asumen los usuarios como consecuencia de dicho uso.
- **c)** Informar de la existencia de controles por parte de la empresa con la intervención mínima necesaria, y solo para aquellos casos especificados.

### OBJETIVO

Establecer los lineamientos para el uso y aprovechamiento del equipo de cómputo, cuidar de la información contenida en los discos de almacenamiento internos, asegurar que los usuarios comprenden la responsabilidad del incumplimiento al presente documento, así como las afectaciones a terceras personas de las que se conservan datos personales.

### Alcance

La aplicación de esta política es de control interno y aplica a todos los empleados que se les haya asignado un equipo de cómputo para el desempeño de sus labores.

### Vigencia

Este documento entra en vigor a partir de su autorización y su vigencia es por tiempo indefinido, debiendo adecuarse a los cambios y a las necesidades de la empresa y a las tecnologías emergentes.

## Disposiciones Generales

### Equipo de cómputo

Se entiende como equipo de cómputo el dispositivo informático que le haya sido asignado al usuario para el desempeño de sus funciones laborales, el cual puede ser una tableta, iPad, laptop o computadora de escritorio.

#### *Del lugar de trabajo*

Se determina como lugar de trabajo las instalaciones de la empresa. Sin embargo, los empleados que realicen labores de campo con el uso de dispositivos móviles, deberán tener los mismos cuidados y apegarse a las mismas condiciones de uso que se describen en general para el uso de equipo de cómputo.

#### *Propiedad del equipo y del contenido*

La empresa es la propietaria del equipo de cómputo, así como de toda la información que contenga en los medios de almacenamiento. Por tal motivo, el usuario deberá evitar hacer uso del mismo para almacenar archivos personales como imágenes, música, documentos, etc.

En caso de que cuando se realicen los mantenimientos programados, el departamento de sistemas detecte la existencia de material personal, pedirá al usuario que en el momento realice el respaldo de los mismos, y posteriormente, procederá a eliminarlos del equipo, previa documentación de lo sucedido.

En ningún caso la empresa pide a los usuarios que presten sus equipos personales para el desempeño de sus funciones, por tal motivo, la empresa no implementa medidas de seguridad bajo la política BYOD *(Bring Your Own Device),* en tal sentido, los equipos personales no podrán conectarse a la red de *Internet,* ni a la red de datos de la empresa.

*USO DEL EQUIPO DE CÓMPUTO*

El equipo deberá usarse únicamente para cumplir con las obligaciones laborales y aquellas que el superior jerárquico determine.

El usuario es responsable de mantener en buenas condiciones el equipo y sus accesorios, de tal manera que, debe evitar tener alimentos en el escritorio, líquidos que puedan derramarse, así como dispositivos magnéticos que puedan afectar el funcionamiento de los discos duros de los equipos de cómputo.

Cuando el usuario detecte alguna anomalía en el equipo, deberá dar aviso de inmediato al Departamento de Sistemas, para que se proceda a dar solución al mismo antes de que ocasione daños mayores.

*SEGURIDAD DE LA INFORMACIÓN*

La modalidad más utilizada para vulnerar los sistemas de información es mediante la ingeniería social, por tal motivo, el usuario deberá mantener confidencial su clave de inicio de sesión, no la deberá compartir con compañeros de trabajo ni usar claves fácilmente deducibles.

Respecto al uso de *Internet,* el usuario debe ser consciente de los sitios que visita, evitando en la medida de lo posible acceder a sitios de dudosa reputación, verificar que accedió al sitio correcto y no a una copia falsa, y ante la duda de la autenticidad y/o seguridad del sitio, solicitar el apoyo al Departamento de Sistemas.

En relación al uso del correo electrónico, el usuario deberá apegarse a las políticas del uso de correo electrónico, además deberá tener el cuidado de no abrir archivos adjuntos de procedencia dudosa, ante la duda, debe solicitar apoyo del Departamento de Sistemas.

Queda estrictamente prohibido que el usuario instale software sin la autorización del Departamento de Sistemas, ya que esto podría ocasionar huecos de seguridad que podrían vulnerar los sistemas de tratamiento de datos personales. Cuando requiera de algún software en específico, deberá solicitar al Departamento de Sistemas la instalación del mismo.

El equipo de cómputo debe tener una cuenta de administrador para el personal de sistemas, el cual se utiliza para realizar mantenimientos y auditorías periódicas de software.

*CESE DE LA RELACIÓN LABORAL*

Cuando por necesidades de la empresa el empleado tenga que separarse del cargo o tenga que abandonar la empresa, este deberá hacer entrega del equipo de cómputo asignado, así como de los archivos contenidos en el mismo.

Queda estrictamente prohibido que el usuario elimine información laboral antes de entregar el equipo de cómputo, ya que al hacerlo podría estar incurriendo en un delito.

Respecto a la contraseña, se recomienda que entregue el equipo sin contraseña para que el Departamento de Sistemas realice las acciones pertinentes de respaldo, limpieza y entrega al nuevo resguardante del equipo.

Lugar y fecha

## ANEXO 4

## CURSO: INTRODUCCIÓN A LA PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES

### OBJETIVO GENERAL

El participante comprenderá la importancia de la protección de los datos personales en los entornos tecnológicos, identificará los elementos mínimos necesarios que debe contener el aviso de privacidad para que los titulares puedan ejercer su autodeterminación informativa, conocerá los principios, deberes y obligaciones que establece la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* y con base en ello, estará en condiciones de cumplir con las políticas establecidas para la protección de los datos personales en su respectiva área, así como de implementar proactivamente medidas de seguridad personales que coadyuven al cumplimiento del objetivo del documento de seguridad.

### CONTENIDO DEL CURSO

El presente curso se divide en 5 módulos de dos horas cada uno; por cada módulo el participante deberá realizar lecturas relacionadas con la protección de datos personales, revisar las leyes nacionales e internacionales, y entregarán una actividad relacionada a cada lectura para constatar la comprensión de la misma.

| **Módulo** | **Temas** | **Horas** |
|---|---|---|
| **Módulo 1**<br>Introducción | • Breve historia del derecho a la protección de datos personales a nivel internacional.<br>• Reconocimiento constitucional del derecho a la protección de datos personales en México<br>• Privacidad / Intimidad<br>• Generalidades de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento<br>• ¿Qué es un dato personal?<br>• Tipos de datos personales | 2 |

| Módulo | Temas | Horas |
|---|---|---|
| | • Participantes en el tratamiento de datos personales<br>• ¿Qué es el derecho a la protección de datos personales?<br>• Principios, deberes y obligaciones<br>• ¿Qué es la autodeterminación informativa?<br>• Derecho al libre desarrollo de la personalidad<br>• El libre desarrollo de la personalidad y la protección de datos personales<br>• Dignidad humana y autodeterminación informativa | |
| **Módulo 2**<br>Tratamiento de datos personales | • Que es el tratamiento de datos personales<br>• Tipos de tratamiento de datos personales<br>• Requerimientos para el tratamiento de datos personales<br>• TI y tratamiento de datos personales<br>• Flujo transfronterizo de datos personales<br>• Transferencias de datos personales<br>• Implicaciones del uso de la nube<br>• Identificación de sistemas de tratamiento de datos personales<br>• Tratamiento de datos personales digitales<br>• Tratamiento de datos personales en físico | 2 |
| **Módulo 3**<br>Procedimientos para el ejercicio de los derechos | • Elementos del aviso de privacidad<br>• Derechos de los titulares<br>• Procedimiento para el ejercicio de los derechos ARCO<br>• Plazos para dar respuesta a los titulares<br>• Violaciones del derecho a la PDP<br>• Procedimientos ante el INAI<br>• Plazos del procedimiento del INAI<br>• Motivos de sanción<br>• Montos de las sanciones<br>• Penas de prisión<br>• Acciones que motivan las penas de prisión<br>• Medios de impugnación | 2 |

| Módulo | Temas | Horas |
|---|---|---|
| **Módulo 4**<br>El documento de seguridad de datos personales | • Que es el documento de seguridad de datos personales<br>• Principales elementos que debe contener el documento de seguridad<br>• Sistema de Gestión de Seguridad de Datos Personales<br>• Normatividad aplicable<br>• Metodologías aplicables<br>• Designación de responsables<br>• Presentación del responsable de datos personales<br>• Presentación de políticas internas<br>• Presentación del inventario de datos<br>• Presentación del resultado del análisis de riesgo | 2 |
| **Módulo 5**<br>Gestión del riesgo | • Obligaciones de los responsables de la protección de datos personales<br>• Análisis de brecha de datos<br>• Implementación de medidas de seguridad<br>• Autorregulación vinculante<br>• Códigos de buenas prácticas en la seguridad de la información<br>• Uso responsable del correo electrónico<br>• Identificación de necesidades | **2** |
| | **HORAS TOTALES:** | **10** |