UNIVERSIDAD MICHOACANA DE SAN NICOLÁS DE HIDALGO

FACULTAD DE DERECHO Y CIENCIAS SOCIALES

DIVISIÓN DE ESTUDIOS DE POSGRADO

MAESTRÍA EN DERECHO DE LA INFORMACIÓN

MANUAL TÉCNICO- JURÍDICO PARA IMPLEMENTACIÓN DE LOS REQUISITOS PREVISTOS EN LA LEY FEDERAL DE PROTECCIÓN DE DATOS EN POSESIÓN DE LOS PARTICULARES EN LOS SUJETOS OBLIGADOS

TESIS

que para obtener el grado de Maestro en Derecho de la Información presenta:

Alumno

Edgar Rodríguez González

Asesor
Doctor en Gobierno y Política Benjamín Revuelta Vaquero

Morelia, Michoacán, Agosto de 2014.

ÍNDICE

CAPÍTULO CUARTO

Implementación de directrices de Datos Personales

CAPÍTULO QUINTO

Regulación de la Videovigilancia

RESUMEN

El auge de los avances tecnológicos, el impulso al Derecho de la Información en México y la interrogante en relación al nivel de conocimientos de la ciudadanía en lo que respecta a la protección de sus datos personales y exigir su derecho a la privacidad, también conocidos como derechos ARCO, da como resultado el presente manual técnico- jurídico, que pretende aportar a la sociedad una guía práctica, en la que se expondrá las reglas procesales, etapas, términos y partes que intervienen, sin dejar de lado elementos doctrinales, procesales y académicos en materia de protección de datos, con la finalidad de garantizar al ciudadano común y a estudiosos del Derecho bases más profundas y útiles en la materia.

PALABRAS CLAVE

Derecho de la Información, protección de datos, derecho a la privacidad, guía práctica, ciudadano común.

ABSTRACT

With the peak of technological advancements, the impulse of the right to information in Mexico and the question in regards to the level of knowledge of the general public and the protection of their personal information and to demand their rights to privacy, also known as ARCO rights, give as a result, this legal- technical manual which aims to provide society with a practical guide in which procedural rules, stages, terms and parties involved will be discussed, without ignoring doctrinal, procedural and academic elements relating to data protection, with the finality to guarantee the common citizen and students of law deeper bases that are useful in the field.

KEY WORDS

Right to information, data protection, rights to privacy, practical guide, common citizen.

INTRODUCCIÓN

La protección de los datos personales en México es un tema sumamente novedoso. Ello derivado del reciente marco jurídico que se ha decidido instrumentar para la defensa y protección de un derecho fundamental. Lo anterior tiene objetivo principal la salvaguarda de mecanismos que garanticen la autodeterminación informativa mediante el establecimiento de tutela efectiva de ciertos derechos de la personalidad que el Estado está obligado a patrocinar en aras de proteger la esfera de la privacidad y la intimidad de las personas. Los grandes retos que se presentan por el vertiginoso desarrollo de la tecnología que atienden principalmente al cumplimiento de las exigencias de los procesos de globalización. La protección de los datos personales han evolucionado al grado de considerarse fundamentales para satisfacer los retos que presentan la sociedad de la información.

Luego entonces, es imprescindible impulsar los conocimientos, derechos y obligaciones, ejes rectores y de trámite que en materia de protección de datos deben de conocer todos los ciudadanos, en especial aquellos relativos a los derechos de Acceso, Rectificación, Cancelación y Oposición (en lo sucesivo ARCO) de sus datos personales que recaben y traten los entes particulares, ya sean personas físicas o morales. Es de considerar también, que la presente investigación pretende aportar los elementos jurídicos procedimentales así como las medidas e información necesaria para la adecuación y el tratamiento de datos conforme a lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en lo sucesivo LFPDPPP). Por lo tanto la presente investigación, con sus respectivos anexos, así como el apartado práctico puede considerarse como una guía para gestionar denuncias por alguna infracción o incumplimiento, conteniendo también elementos doctrinales, procesales y conceptos generales. Adicionalmente, se establecen los actos y procedimientos administrativos relativos a las facultades de verificación y el ejercicio de la potestad sancionadora por parte del Instituto Federal de Acceso a la Información Pública y Protección de Datos (en lo sucesivo IFAI), en su calidad de

autoridad garante en materia de protección de datos personales en posesión de los particulares hacia los sujetos regulados.

En otro orden de ideas y derivado de la reciente entrada en vigor de la LFPDPPP y su Reglamento y su nacimiento a la vida jurídica en México se ha generado como un esquema garante de protección en materia de datos personales. Es por ello que debemos preguntarnos: ¿La ciudadanía tiene el nivel adecuado de conocimiento de los derechos subjetivos que existen para proteger sus datos personales y los procedimientos para exigir su derecho a la privacidad que en la vía administrativa pueden ejercitar ante la autoridad en la materia?. Ante tal interrogante surge la inquietud de elaborar la presente investigación. Ello tiene como finalidad que las personas conozcan de una manera más amplia la defensa eficaz de sus datos personales frente a las empresas que están obligadas a respetar la autodeterminación informativa.

Una razón adicional de profundizar en este tema es la particularidad que México tiene en la materia de acuerdo a los resultados de la "Encuesta Nacional sobre Protección de Datos Personales a Sujetos Regulados por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) y Población en General"[1], de la cual un 75 % no conoce o ha escuchado algo sobre la LFPDPPP. Sin embargo, 8 de cada 10 entrevistados consideran muy o algo importante que las empresas puedan suprimir o eliminar sus datos personales cuando termina su relación con éstas. Adicionalmente, se determino que si bien 3 de cada 10 personas señalaban al IFAI como institución garante de la Ley, esta proporción se reduce a 2 de cada 10 cuando se trataba de identificar al IFAI como la instancia a la cual pueden acudir en caso de que un particular no atienda sus solicitudes de derechos de acceso, rectificación y oposición de sus datos personales. Es de considerar también que el 84% de las empresas desconoce las obligaciones de la LFPDPPP. Consecuentemente el 69% de los sujetos regulados están dispuestos a colaborar y ser capacitados por el IFAI para implementar las acciones necesarias para la protección de los datos personales que tratan. Asimismo el 76% de los sujetos regulados ignora las

[1] Encuesta realizada por la empresa Ipsos Public Affairs para el Instituto Federal del acceso a la información pública y protección de datos en 2012. Preparado para la Secretaría de Protección de datos mediante diversas entrevistas efectivas a hombres y mujeres de 12 años o más y sujetos obligados de diferentes sectores económicos. Consultada el día 27 de Mayo de 2013. Disponible en línea en la siguiente dirección electrónica: http://inicio.ifai.org.mx/DocumentosIMGSlider/EncuestasNacionalPDP2012.pdf

consecuencias de no cumplir con las disposiciones de la Ley. Por último, y como una justificación más para desarrollar la descripción y defensa de la protección de datos personales en posesión de los particulares es la que concluye que 7 de cada 10 sujetos obligados consideran que la LFPDPPP tiene muchísima o mucha utilidad.

En México existen relativamente pocos referentes en los cuales el ciudadano común pudiera consultar como para guiarse en la protección de sus datos personales.de la presente investigación son los escasos procedimientos de verificación y de imposición de sanciones que se encuentran documentados en México, los cuales aproximadamente no exceden de cinco casos en el 2012.[2]

Ahora bien, atendiendo a una de las recomendaciones de la citada encuesta que en cierto modo es catalogada por los especialistas como prioritaria es aquella en la que se sugiere que se debe de dotar a la población en general de los conocimientos y herramientas mínimas en la materia. Lo anterior establece las condiciones necesarias para las personas estén en posibilidades de actuar de manera preventiva ante una posible verificación de la autoridad. Es más se deben enfocar las acciones de manera particular en el conocimiento de los derechos ARCO, su ejercicio, medios de defensa disponibles y autoridades a las cuales pueden acudir para hacer efectivo este derecho.

Es de especial consideración también el hecho de desarrollar la protección de datos personales para obtener conocimientos específicos en una de las ramas del Derecho a la Información. Ahora bien, otro de los fines ulteriores de lo expuesto en los presentes capítulos es aplicación de los contenidos en el ámbito profesional, especialmente para coadyuvar en el tramitación y ejercicio de los derechos ARCO de los interesados o afectados que así lo soliciten. Igualmente se podrá contar con los elementos jurídicos que consolidan la formación en una de las áreas del derecho administrativo en cuanto a los elementos procesales y formales del procedimiento de verificación, y las facultades sancionadoras del IFAI. En consecuencia aporta los elementos especiales para ser un

[2] Esta afirmación se realiza en base a la información generada por el Instituto Federal del acceso a la información pública y protección de datos en 2012. Consultada el día 13 de Junio de 2012. Disponible en línea en la siguiente dirección electrónica: http://consultas.ifai.org.mx/SesionesspDP

conocedor o técnico en la protección y defensa de los datos personales frente a los particulares.

La presente investigación auxilia a enriquecer los conocimientos académicos en materia de protección de datos personales, ya que son escasos los estudios realizados bajo la perspectiva aquí planteada. También debemos considerar que realmente en México existen pocos académicos que tienen injerencia en los temas aquí expuestos, así como el insuficiente material de consulta.

Atendiendo a la necesidad de los planteamientos y razones antes expuestas el presente manual técnico nace de la especial necesidad de contar un instrumento guía que sirva como referencia para aquellos que pretenden adquirir conocimientos más profundos en la materia. Es decir en la medida del espectro de difusión que se tenga de los contenidos que se abordarán aquí coadyuvarán para que los responsables del tratamiento de datos, personas físicas, representantes legales, abogados, académicos y todos aquellos interesados en adquirir profundos conocimientos en los procedimientos jurídico-administrativo en protección de datos personales en posesión de los particulares. Incluso cuando los ciudadanos ejercen sus derechos para la defensa de sus intereses personales o patrimoniales en materia de datos personales. Es por ello, que se expondrán las reglas procesales, etapas, términos, actuaciones, partes que intervienen y distintas consideraciones sobre los actos de trámite, así como formularios que facilitan la aplicación de las normas reguladoras en materia de protección de datos.

En otro orden de ideas, la metodología bajo la cual se desarrolla la presente investigación es de carácter dogmática y estudio normativo basada principalmente en elementos documentales de tipo bibliográfico y de expedientes administrativos en la que utilizaremos los métodos inductivo, deductivo, el análisis, la síntesis y el comparativo. Así también atenderemos parcialmente al derecho comparado particularmente en lo que se refiere a la legislación española. Igualmente se abordarán los lineamientos establecidos en el método jurídico para establecer un proceso lógico deductivo orientado a una propuesta jurídico-administrativa para dotar de un esquema más funcional en materia de protección de datos personales en posesión de los particulares. Cabe mencionar que en

esta investigación se profundizará en las fuentes de información desde un punto de vista cualitativo ello con la finalidad de que la información que se obtenga sea confiable y útil.

La justificación del uso de los métodos enunciados en el párrafo anterior se debe a que la utilización de los mismos facilita el diseño y explicación del procesamiento de datos de la presente investigación; así también consolida el proceso racional más optimo el cual nos auxiliará a comprobar el logro de los objetivos a comentar y desarrollar.

El tipo de investigación utilizada es la jurídico-descriptiva ya que se identifican cada una de las etapas del los distintos procedimientos establecidos para garantizar la tutela efectiva de derechos en protección de datos personales, las fases de los procedimientos de verificación y de sanción los cuales son incoados frente a los sujetos regulados por parte de la autoridad administrativa facultada para su aplicación.

Los recursos disponibles para el desarrollo de la presente investigación han sido los suficientes para asegurar la conclusión de la misma, pues se ha procurado recopilar fuentes de información especializadas como bibliográficas, hemerográficas, diccionarios, enciclopedias, sentencias, legislaciones, distintos recursos cibernéticos, cursos especializados en la materia, entrevistas con destacados especialistas en protección de datos. Más aun es de considerar las estancias de investigación en organismos académicos especializados como es la Facultad de Ciencias de la Información y la Facultad de Derecho de la Universidad Complutense de Madrid, así como en la Agencia de Española de Protección de Datos Personales.

Ahora bien con el resultado de la presente investigación los sujetos obligados y los titulares de los datos personales conocerán los elementos legales y procesales para ejercer y respetar el control y tratamiento de los datos personales. Puesto que se analizarán y desarrollarán de manera detallada definiciones, explicación de procedimientos, así como resoluciones destacadas de cada uno de los derechos ARCO. Así también se abordarán las

disposiciones jurídicas establecidas en la Ley Federal de Protección de Datos Personales, su Reglamentos y otras disposiciones de carácter normativo.

En consecuencia las empresas y particulares contaran con un referente confiable para implementar un procedimiento conforme a la normatividad aplicable, con el objeto de obtener para obtener la autorización de las personas para accesar, recabar, tratar, transferir o cancelar datos personales.

Sin embargo, es de considerar que el principal objetivo del contenido del presente trabajo, es el de conocer el control de legalidad que debe prevalecer sobre el cumplimiento a las disposiciones de la LFPDPPP y su Reglamento. Luego entonces los titulares de los datos personales y los sujetos regulados ya sea el responsable o encargado del tratamiento de datos personales, observarán en todo momento los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad en el tratamiento de los mismos.

En otro orden de ideas, se utilizaron fuentes de información como bibliografía especializada en materia de protección de datos personales, memorias, artículos de revistas especializadas, resoluciones administrativas emitidas por autoridades en materia de protección de datos personales, guías, documentos electrónicos, diversas legislaciones y reglamentos, información obtenida de páginas web. Incluso se considero de forma especial las aportaciones de José López Calvo en su texto intitulado "*Actividad inspectora y procedimiento administrativo sancionador en materia de protección de datos personales*", en el libro "La potestad sancionadora de la Agencia Española de Protección de Datos". Cabe destacar también la información documental de la Agencia Española de Protección de Datos, así como los textos especializados en los repositorios de la facultad de ciencias de la Información y de Derecho de la Universidad Complutense de Madrid, así como la acertada tutoría del Dr. Héctor Pérez Pintor, la Dra. Pilar Cousido González y el Dr. Benjamín Revuelta Vaquero en el desarrollo del presente trabajo

Es de valorar también los anexos de la presente investigación los cuales principalmente están constituidos por una serie de formatos y formularios en materia de protección de datos personales los cuales se encuentran debidamente estructurados y fundamentados los

cuales podrán ser utilizados tanto por los titulares de los datos para ejercer su autodeterminación informativa frente a los sujetos regulados, adicionalmente se encuentran algunos formatos de documentos de carácter preventivo respecto de un manejo responsable de la información de carácter personal.

De manera concluyente se incluye un procedimiento de solicitud de protección de derechos presentada ante el Instituto Federal de Acceso a la Información y Protección de Datos. En este se refleja una parte práctica de lo desarrollado en los capítulos del presente manual.

CAPÍTULO PRIMERO

El presente Capítulo se refiere al estudio del núcleo de los derechos fundamentales en la protección de datos bajo los cuales el titular de los mismos puede ejercitar un verdadero control directo sobre su información personal ejercicio y tutela de los derechos de acceso, rectificación, cancelación y oposición, frente a quien sea responsable del tratamiento de sus datos. En este capítulo encontraremos definiciones de cada uno de los derechos, criterios doctrinales, figuras de derecho comparado con la legislación española, elementos procedimentales de tutela a ejercer ante la instancia correspondiente para actuar ante supuesto de denegación por parte de los sujetos regulados, legislación aplicable, resoluciones administrativas, criterios judiciales y casos prácticos que ayudan a una mejor comprensión de dichas facultades del ciudadano. Asimismo se hará referencia a una figura jurídica intitulada por la legislación reglamentaria en materia de protección de datos personales como "tratamiento de datos personales en decisiones sin intervención humana valorativa", este se refiere a la valoración de perfiles informáticos de los individuos, sin embargo es escasa la información del mismo, por lo que en esta investigación se hará un desarrollo del mismo tomando como referente la legislación española, ya que en la misma se encuentra una institución jurídica de igual naturaleza llamada "impugnación de valores", por lo que del análisis de este último nos ayudará a entender el ejercicio de este derecho tan peculiar.

Procedimiento de tutela efectiva de derechos

1.1. Parte general.

Cuando el titular de sus datos personales realiza el ejercicio de tutela de derechos de acceso, rectificación, cancelación y oposición que realice frente a los sujetos regulados y derivado de ello no recibe respuesta por parte del responsable o del encargado del tratamiento de los datos, o lo haga en un formato incomprensible, se niegue a efectuar la cancelación, modificaciones o correcciones a los datos personales o porque la información

entregada considerara que es incompleta o no corresponda a la información requerida o considera que fue vulnerada alguna disposición prevista en la LFPDPPP, podrá considerar el inicio de un procedimiento de tutela efectiva de derechos ante el IFAI.

1.1.1. Partes en el procedimiento de tutela efectiva de derechos.

Los sujetos principales que podemos identificar como partes dentro del procedimiento de tutela de derechos en materia de protección de datos personales son los siguientes:

1.- Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) la cual tiene la calidad de autoridad administrativa.

2.- Titular de los datos o su representante legalmente debidamente acreditado, el cual tiene la calidad de sujeto activo.

3.- El responsable y en el encargado del tratamiento de los datos o en su caso un tercero que preste los servicios de forma legítima, mimo que tiene la calidad de sujeto obligado o regulado.

4.- Tercero Interesado: En el caso que corresponda sería la persona que acredite el interés jurídico o legitimo para intervenir en el asunto antes del cierre de la instrucción.

1.1.2. Etapas procesales.

1.- El procedimiento de protección de derechos se iniciará por reclamación del afectado ante la autoridad respectiva (IFAI), mediante escrito libre en el que deberá plasmar el contenido de la reclamación y los preceptos normativos que se consideran violados. Para efectos de evitar un posible requerimiento por parte de la autoridad se sugiere que el escrito presente todos los elementos formales que dispone el artículo 46 de la LFPDPPP los cuales a continuación se detallan:

A.- El nombre del titular o, en su caso, el de su representante legal, así como del tercero interesado, si lo hay.

B.- El nombre del responsable ante el cual se presentó la solicitud de acceso, rectificación, cancelación u oposición de datos personales.

C.- El domicilio para oír y recibir notificaciones.

D.-La fecha en que se le dio a conocer la respuesta del responsable,[3] salvo que el procedimiento inicie con base en lo previsto en el artículo 50 de la LFPDPPP;

E.-Los actos que motivan su solicitud de protección de datos, y

F.-Los demás elementos que se considere procedente hacer del conocimiento del Instituto.

En el caso de que la solicitud no presente los requisitos antes mencionados, el IFAI prevendrá al titular de los datos para que en un término de 20 días hábiles siguientes a la presentación de la solicitud y por una sola vez para que subsane la omisiones dentro de un plazo no mayor a cinco días hábiles. En el supuesto de que fenezca el plazo sin que el interesado desahogue la prevención, se tendrá por no presentada la solicitud de protección de datos. Cabe hacer mención que la prevención produce el efecto de interrupción que tiene el IFAI para resolver la solicitud de protección de datos, ello conforme a lo dispuesto en el artículo 49 de la LFPDPPP.

La solicitud en materia de protección de derechos de datos personales podrá presentarse en los siguientes términos:

[3] Conforme a lo dispuesto en el artículo 50 de la LFPDPPP el IFAI podrá suplir las deficiencias de la queja en los casos que así se requiera, siempre y cuando no altere el contenido original de la solicitud de acceso, rectificación, cancelación u oposición de datos personales, ni se modifiquen los hechos o peticiones expuestos en la misma o en la solicitud de protección de datos.

a).- En el domicilio del Instituto.

b).- Oficinas habilitadas que el Instituto determine.

c).- A través de los sistemas que el propio Instituto establezca[4].

d).- Correo certificado con acuse de recibo.

2.-La presentación del escrito con sus correspondientes anexos deberá de realizarse dentro de los 15 días hábiles siguientes a la fecha en que se comunique la respuesta al titular por parte del responsable o la negativa en el caso que corresponda.

3.- Posteriormente se corre traslado al sujeto regulado para que en un término de 15 días emita la respuesta correspondiente, presente las pruebas pertinentes y manifieste lo que a su derecho convenga.

4.-La autoridad desahogará las pruebas que estime pertinentes y procederá a su desahogo, pudiendo solicitar de manera oficiosa aquellas pruebas que estime necesarias. Consecutivamente se le otorga al responsable un término de cinco días posteriores a su notificación para efecto de que realice los alegatos correspondientes.

Los medios de prueba que se podrán ofrecer dentro del procedimiento que nos ocupa son la documental pública, la documental privada, la inspección, siempre y cuando se realice a través de la autoridad competente, la presuncional, en su doble aspecto, legal y humana, la

[4] Cuando el solicitante opte por esta modalidad deberá de contar con la certificación del medio de identificación electrónica a que se refiere el artículo 69-C de la Ley Federal de Procedimiento Administrativo, dicho ordenamiento legal dispone esencialmente lo siguiente: En los procedimientos administrativos, las dependencias y los organismos descentralizados de la Administración Pública Federal recibirán las promociones o solicitudes que, en términos de esta ley, los particulares presenten por escrito, sin perjuicio de que dichos documentos puedan presentarse a través de medios de comunicación electrónica en las etapas que las propias dependencias y organismos así lo determinen mediante reglas de carácter general publicadas en el Diario Oficial de la Federación. En estos últimos casos se emplearan, en sustitución de la firma autógrafa, medios de identificación electrónica.

pericial[5], la testimonial, y las fotografías, páginas electrónicas, escritos y demás elementos aportados por la ciencia y tecnología.

5.- El plazo máximo en que se dicte la resolución en el procedimiento de tutela efectiva de derechos será por un término de cincuenta días hábiles, contados a partir de la fecha de presentación de la solicitud de protección de datos, término que podrá ser ampliado por la autoridad por una sola vez hasta por otros cincuenta días con autorización del pleno.

6.- Si la resolución resulta favorable al titular de los datos se requerirá al responsables para que en un termino de diez días hábiles siguientes a la notificación se haga efectivo el ejercicio de los derechos objeto de su protección.

1.1.3. Tipología de las resoluciones

Dentro de los autos que ponen fin al procedimiento de tutela efectiva de derechos o para el caso que se generen resoluciones por parte del IFAI, estas podrán ser de la siguiente manera:

I.- Sobreseerse por los siguientes motivos:

I.I Muerte del titular.

I.II Desistimiento expreso del titular.

I.III Cuando admitido el procedimiento sobrevenga una causal de improcedencia

I.IV Cuando quede sin materia.

[5] Conforme a lo dispuesto en el artículo 119 del Reglamento de la LFPDPPP para el caso de que se ofrezca prueba pericial o testimonial, se precisarán los hechos precisos sobre los que deban versar y se señalarán los nombres y domicilios del perito o de los testigos, exhibiéndose el cuestionario o el interrogatorio respectivo en preparación de las mismas. Sin estos señalamientos se tendrán por no ofrecidas dichas pruebas.

II.- Cuando se generen las siguientes causas de improcedencia:

II.I.- Cuando el IFAI se declare incompetente.

II.II.- Cuando el IFAI haya conocido con anterioridad de la solicitud en materia de protección de datos contra el mismo y se haya resuelto en definitiva respecto del mismo recurrente.

II.III Cuando se encuentre en trámite algún recurso o medio de defensa ante un tribunal competente interpuesto por el titular de los datos que pueda tener como consecuencia legal modificar o revocar el acto respectivo.

II.IV Cuando la solicitud de datos sea ofensiva o irracional[6]

II.V Cuando se presente de manera extemporánea.

III.- En el caso de que el IFAI desahogue el procedimiento en todas sus etapas, hasta la formulación de alegatos procederá a la emisión del resolutivo el cual podrá confirmar, revocar o modificar la respuesta del responsable de los datos. Es de considerar que en cualquier momento las partes podrán conciliar siendo la autoridad el órgano facultado que concilie los intereses de ambas partes.

1.1.4. Medios de impugnación

Si a consideración del interesado o una de las partes la resolución no satisface el interés jurídico en el procedimiento de protección de derechos procede el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa.

[6] Cabe aclarar que existe una imprecisión de cuales serían datos ofensivos o irracionales, ya que el Reglamento de la LFPDPPP no hace pronunciamiento alguno al respecto.

1.2. Parte especial

En este apartado se desarrollan los aspectos procedimentales y consideraciones particulares del derecho de acceso, rectificación, cancelación y oposición en materia de protección de datos, ya que cada uno de ellos esta matizado por elementos específicos que caben mencionar de manera desglosada y puntual.

1.2.1 Derecho de acceso

El derecho de acceso consiste en la facultad que tienen todas aquellas personas para acceder a los registros y a los documentos que forman parte de un expediente que obren en los archivos de entidades privadas. Toda vez que se encuentren en ellos datos de carácter personal cualquiera que sea la forma de expresión, gráfica, sonora e imagen, o el tipo de soporte material en que figuren.[7]

Por medio del derecho de acceso, el responsable del tratamiento de los datos está obligado a atender la solicitud de información que le solicite el titular de los datos personales[8]. Ahora bien es de considerar que el derecho de acceso en el tratamiento de los datos personales implica también el conocimiento de la lógica utilizada en los mismos, la categoría de los datos a que se refiere y la comunicación que de estos se haya realizado, o las que se prevén realizar a terceros y los destinatarios de las mismas.[9]

El derecho de acceso a los datos personales de acuerdo a los Estándares Internacionales sobre Protección de Datos Personales y Privacidad consiste en que:

---

[7] DEL PESO Emilio, RAMOS Miguel Ángel, DEL PESO Margarita. *Nuevo Reglamento de Protección de Datos de Carácter Personal*. España. Ediciones Díaz de Santos. 2008. 110 p.

[8] TASCÓN Rodrigo. *El tratamiento por la empresa de datos personales de los trabajadores, Análisis del estado de la cuestión*. España. Editorial Aranzandi. S.A. 2005. 94 p.

[9] TELLEZ Abel. *Nuevas Tecnologías. Intimidad y Protección de datos*. España. Edisofer S.A. 2001. 161 p.

"El interesado tendrá derecho a recabar de la persona responsable cuando así lo solicite, información relativa a los concretos datos de carácter personal objeto de tratamiento, así como al origen de dichos datos, a las finalidades de los correspondientes tratamientos y a los destinatarios o las categorías de destinatarios a quien se comuniquen o se pretendan comunicar".[10]

Este derecho cobra especial interés en algunos supuestos en que el mismo titular de los datos desconoce parte de su vida propia, como puede ser en algún caso de amnesia, perdida de la memoria, búsqueda de la paternidad o maternidad biológica, datos de la niñez que pueden obrar en una institución académica, algún centro social o de atención a la infancia y en otros casos más extremos los datos relativos a la filiación e identificación del origen del adoptado tal como se establece en la sentencia emitida por el Tribunal Europeo de Derechos Humanos caso Gaskin vs Reino Unido del 7 de Julio de 1989.[11]

1.2.1.1. Procedimiento para el ejercicio del derecho de acceso

Inicialmente el titular de los datos o su representante legal solicitará el ejercicio del derecho de acceso al responsable del tratamiento de los datos personales que le conciernen debiendo considerar el estricto cumplimiento de los elementos formales que establece el artículo 29 de LFPDPPP los cuales se transcriben a continuación:

A).- El nombre del titular y domicilio u otro medio para comunicarle la respuesta a su solicitud.

[10] Estándares Internacionales sobre Protección de Datos Personales y Privacidad. Resolución de Madrid. *Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad en relación con el tratamiento de Datos de Carácter Personal* .Conferencia Internacional de Autoridades de Protección de Datos y Privacidad 5 de Noviembre de 2009**.**

[11] Gaskin contra Reino Unido. Serie A, número 160 (TEDH 1989 16; JUR 2001, 598).Esta sentencia examino el caso del Sr. Gaskin quien desde pequeño fue confiado a la asistencia social, posteriormente quiso acceder a su expediente confidencial custodiado por las autoridades locales, en el que incluía informes de todas las personas que habían intervenido en su acogimiento infantil. No pudiendo acceder a la totalidad de su expediente ya que cierta información fue recabada bajo secreto, el interesado apeló ante el Tribunal de Estrasburgo, por lo que esté estimo la existencia de un interés vital Gaskin en recibir la información necesaria para conocer y comprender su infancia y las etapas de su desarrollo, concluyendo en la protección del citado interés.

B).- Los documentos que acrediten la identidad o, en su caso, la representación legal del titular.

C).- La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno del derecho de acceso.

D).- Cualquier otro elemento o documento que facilite la localización de los datos personales.

El derecho de acceso es de carácter personalísimo, siendo ejercido directamente por el interesado debiendo utilizar cualquier medio que permita acreditar el envió y la recepción de la solicitud. Así también se debe facilitar el ejercicio de este derecho mediante medios telefónicos en los que deberá solicitarse información que pueda ser conocida por el titular de los datos considerando que el resultado deberá enviarse al domicilio que el titular señale[12].

El consentimiento es un requisito indispensable para que el titular de los datos obtenga la información del cual tiene conocimiento sobre la información que está siendo tratada. Sin embargo puede presentarse la circunstancia de que se esté tratando información sin que el titular de los datos tenga conocimiento de ello. Por lo tanto la LFPDPPP protege a los titulares de los datos personales para efecto de que los sujetos obligados no acumulen información del perfil de la personalidad del individuo.[13]

El Reglamento de la LFPDPPP conforme a lo dispuesto en su Artículo 101 en cuanto al derecho de acceso establece textualmente lo siguiente:

[12] CASTAÑEDA, Alberto y BONADEO Rodrigo. *Guía práctica de protección de datos de carácter personal*. España. Ediciones Experiencia S.L., 2002. 149 p.
[13] Ídem.

"*El titular, en términos de lo dispuesto por el artículo 23 de la Ley, tiene derecho a obtener del responsable sus datos personales, así como información relativa a las condiciones y generalidades del tratamiento*."

Dicha solicitud deberá presentarse con el responsable del tratamiento de los datos personales o con la persona que se haya designado para tal efecto. Posteriormente el responsable contará con un plazo máximo de veinte días hábiles computados a partir de la fecha en que se recibió la solicitud de acceso. Toda vez que deberá comunicarse la procedencia o negativa del derecho de acceso para que en el caso de que se cuente con datos personales se haga efectiva la comunicación de los mismos dentro de los quince días hábiles siguientes a la notificación. Cuando se entregue la información por parte del responsable al titular de los datos obligatoriamente se deberá acreditar la identidad del solicitante o del representante legal según corresponda.

Es de considerar que los plazos anteriormente referidos podrán ser ampliados por una sola vez por un periodo igual siempre y cuando se justifique plenamente por parte del titular de los datos.

Mediante el ejercicio del derecho de acceso el titular de los datos obtiene información exacta, veraz y de forma gratuita respecto de los siguientes aspectos:[14]

1.- Los datos de carácter personal sometidos a tratamiento.

2.- El origen de los datos.

3.- Las cesiones o comunicaciones realizadas o que se prevé realizar a terceros.

Se debe de establecer un mecanismo para que el afectado pueda optar en el ejercicio de su derecho de acceso a le faciliten varios medios o sistemas de consulta. Ahora bien siempre

[14] CASTAÑEDA, Alberto y BONADEO Rodrigo. Ref.12. 148 p.

se debe considerar la salvaguarda de información de los derechos de terceros y la configuración o implementación del material del fichero o la naturaleza del tratamiento de los datos que permitan establecer medidas de seguridad idóneas.[15]

Al ejercitar el derecho de acceso el responsable del tratamiento de los datos deberá considerar que cualquier información que se proporcione al interesado deberá facilitarse de forma inteligible debiendo emplear para ello un lenguaje claro y sencillo.[16] Por lo antes expuesto el titular del derecho de acceso podrá recibir su información personal a través de las siguientes formas:[17]

1.- Escrito, copia, fotocopia remitida por correo certificado con acuse de recibo.

2.- Fax.

3.- Correo electrónico u otros sistemas de comunicaciones electrónicas.

4.- Cualquier otro sistema que sea el adecuado según el responsable del fichero para el correcto manejo de la información.

Para el caso de que sea procede el derecho de acceso únicamente se entregará la información a quien legítimamente se encuentra facultado para ello. Inicialmente será el titular de los datos o a quien legalmente lo acredite en términos del artículo 32 de la LFPDPPP, mismo que a la letra dice:

> *" …Tratándose de solicitudes de acceso a datos personales, procederá la entrega previa acreditación de la identidad del solicitante o representante legal, según corresponda. "*

En otro orden de ideas se puede presentar la circunstancia en la que el titular de los datos personales puede acudir al sitio físico en donde se encuentra la información a

---

15 VELEIRO Belen. *Protección de datos de carácter personal y sociedad de la información*. Madrid. Boletín Oficial del Estado.2008. 92 p.

16 Estándares Internacionales sobre Protección de Datos Personales y Privacidad. Resolución de Madrid. Ref. 10.

17 Agencia Española de Protección de Datos. *El derecho fundamental a la protección de datos: Guía para el ciudadano*. [En línea]. España 2011. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_CIUDADANO_OK.pdf. 25 p.

criterio del responsable del tratamiento de los datos, tal y como lo dispone el artículo 99 de la LFPDPPP mismo que textualmente cita lo siguiente:

> *"Cuando el acceso a los datos personales sea en sitio, el responsable deberá determinar el periodo durante el cual el titular podrá presentarse a consultarlos, mismo que no podrá ser menor a quince días. Transcurrido ese plazo, sin que el titular haya acudido a tener acceso a sus datos personales, será necesaria la presentación de una nueva solicitud."*

El responsable del tratamiento de los datos deberá cumplir estrictamente con lo que dispone la LFPDPPP y su reglamento al facilitar el acceso, los requerimientos y medidas de seguridad oportunas. Sin embargo, si el responsable del tratamiento ofreciera un determinado sistema para hacer efectivo el derecho de acceso y el titular de los datos lo rechazase, aquél no responderá por los riesgos que para la seguridad de la información pudieran derivarse de la elección.[18] No obstante, el responsable del tratamiento de los datos podrá apoya en todo momento al titular de los datos para que pueda subsanar algún defecto que pueda presentar en su solicitud de acceso.

En virtud del derecho de acceso se puede considerar que el responsable del tratamiento de los datos puede establecer procedimientos diversos para hacer efectivo el derecho de acceso. Sin embargo, si el titular de los datos exigiese que el mismo debe materializar a través de un procedimiento que implique un gasto desproporcionado con el mismo efecto y garantizando igual seguridad, serán de su cuenta los gastos derivados de su elección.[19] Por lo antes expuesto, y con el ánimo de optimizar y agilizar el derecho de acceso el artículo 89 Fracción I de la LFPDPPP la cual permite establecer medios de autentificación de tipo electrónico o firma electrónica avanzada.

Por razones de especial complejidad cuando sea necesario el responsable del fichero podrá solicitar del afectado la especificación de los ficheros sobre los cuales quiera

[18] VELEIRO Belén. Ref. 15. 93 p.
[19] Ídem.

ejercitar el derecho de acceso, por lo tanto se deberá de facilitar una relación de todos ellos.[20]

El acceso a los documentos que contengan datos referentes a la intimidad de las personas estará reservado a estas y en el supuesto de observar que tales datos figuran incompletos o inexactos podrán exigir que sean completados o rectificados, salvo que figuren en expedientes caducados.[21] No obstante lo anterior, debemos de considerar que es indiferente el derecho de acceso en cuanto al tipo de información al que se pretenda obtener pues el mismo trato que debe darle el responsable del tratamiento de los datos personales especialmente protegidos o datos meramente identificativos, ya que todos los datos que identifiquen a una persona o que la hagan identificable son datos personales.[22]

En el caso de que el titular solicite el acceso a los datos a una persona que presume es el responsable y ésta resulta no serlo bastará con que así se le indique al titular por cualquiera de los medios a que se refiere el párrafo anterior y por tanto se considera por cumplida la solicitud como lo dispone el artículo 33 de LFPDPPP.

1.2.1.2. Causales de negativa al derecho de acceso

Conforme a lo dispuesto en el artículo 34 de la LFPDPPP el responsable podrá negar el acceso a los datos personales en los siguientes supuestos:

A).- Cuando el solicitante no sea el titular de los datos personales o el representante legal no esté debidamente acreditado para ello.

B).- Cuando en su base de datos no se encuentren los datos personales del solicitante.

C).- Cuando se lesionen los derechos de un tercero.

[20] Ibídem.. Ref. 15. 92 p.
[21] DEL PESO Emilio, Ref. 07. 110 p.
[22] TASCÓN Rodrigo. Ref. 08. 94 p.

D).- Cuando exista un impedimento legal o la resolución de una autoridad competente restrinja el acceso a los datos personales.

E).- Cuando la cancelación haya sido previamente realizada.

La negativa por parte del responsable de los datos a la persona que sea designada para ello podrá ser parcial en cuyo caso el responsable efectuará el acceso requerido por el titular.

En todos los casos anteriores el responsable deberá informar el motivo de su decisión y comunicarla al titular o en su caso al representante legal en los plazos establecidos para tal efecto ya sea por el mismo medio por el que se llevó a cabo la solicitud, acompañando en su caso las pruebas que resulten pertinentes.

1.2.1.3. Plazos para el ejercicio del derecho de acceso

En la legislación mexicana al igual que otras legislaciones como la española se contempla el ejercicio del derecho de acceso por parte del interesado el cual podrá ejercerlo de manera gratuita en intervalos de 12 meses. Sin embargo, puede representar un costo para el titular de los datos para ejercer su derecho de acceso en México. Ello, en virtud de que el artículo 35 párrafo segundo de la LFPDPPP, dispone que si el titular del derecho, reitera el acceso a la información en un periodo menor a doce meses. Asimismo se deberá considerar que los costos no serán mayores a tres salarios mínimos vigentes en el Distrito Federal a menos que existan modificaciones sustanciales al aviso de privacidad.

Es de hacer notar lo establecido en los Estándares Internacionales sobre Protección de Datos Personales y Privacidad o la llamada Resolución de Madrid para ejercer el derecho de acceso a los datos personales en periodos inferiores a doce meses el cual se transcribe a continuación:

> *"La legislación nacional aplicable podrá limitar el ejercicio reiterado de estos derechos, que obligaría a la persona responsable a responder múltiples solicitudes en intervalos cortos de tiempo, excepto en aquellos casos en los que el interesado haga constar en su solicitud un interés legítimo."*

Para ejercer el derecho de acceso vía excepción antes de los doce meses referidos en el párrafo anterior, mediante la manifestación de un interés legitimo que se puede alegar para ejercer el derecho de acceso más de una vez al año, será aquel en que se demuestre que se están sometiendo más datos a tratamiento que los que efectivamente se han comunicado al interesado en el ejercicio anterior de su derecho de acceso.[23]

1.2.1.4. Excepciones al derecho de acceso

Es de considerar que en algún momento vía excepción el ejercicio al derecho de acceso se puede limitarse en el supuesto que los datos se encuentren bloqueados y no estén sujetos a tratamiento. Por lo que, para todos los efectos deberán ser considerados como cancelados, por tanto el derecho de acceso es improcedente[24]. Adicionalmente los sistemas de consulta del fichero previstos para el ejercicio del derecho de acceso podrán ser restringidos en función de la configuración o implantación material del fichero o de la naturaleza del tratamiento, siempre que en que ofrezca al afectado sea gratuito y asegure la comunicación escrita si éste así lo exige.[25]

La denegación al derecho de acceso se actualizara cuando la solicitud sea formulada por persona distinta del afectado y no se acreditase que la misma, se deberá probar que se actúa en representación de aquel.[26] Cabe la posibilidad de que vía excepción al carácter personalísimo de los derechos de acceso puede proceder mediante la representación del titular de los datos por encontrarse en incapacidad legal o por ser menor de edad. Esta situación deberá acreditarse en la solicitud de acceso que se presente al sujeto obligado.

---

[23] TASCÓN Rodrigo. Ref. 08. 95 p.

[24] COUDERT Fanny. Ejercicio de Derechos. En: ALMUZARA Cristina: *Estudio práctico sobre la protección de datos de carácter personal*. España. Editorial LEX NOVA S.A. 2005. 371 p.

[25] VELEIRO Belén. Ref. 15. 93 p.

[26] DEL PESO Emilio, Ref. 07. 118 p.

1.2.1.5. Resoluciones destacadas en materia del derecho de acceso

En cuanto al derecho de acceso por parte de los titulares de los datos personales podemos mencionar la resolución: R/00372/2013 emitida por la Agencia Española de Protección de Datos Personales en la que el titular de los datos solicita su derecho de acceso a la empresa GOOGLE SPAIN S.L. el estadístico de las direcciones IP y las fechas en las que han accedido a GOOGLE SPAIN S.L. consultando el nombre del titular de los datos motivo del ejercicio. Ahora bien con ello se pretende generar un estadístico y determinar si alguien estuvo detrás de actividades fraudulentas. La agencia resuelve que es inadmisible la petición del titular de los datos en razón de que la pretensión del mismo no es accesar a sus datos personales, si no obtener información de terceros.[27]

La resolución R/00475/2011 igualmente emitida por la Agencia Española de Protección de Datos Personales en la que el titular de los datos personales ante la empresa denominada ASESORÍA CEDRÉS, S.L. solicitó diversa documentación en la que figura como titular la cual posee por la relación contractual que existió entre las partes. Dicha información consiste en facturas de proveedores de varios años y justificantes de pagos de impuestos de diferentes años. Sin embargo, el criterio que se estableció en el resolutivo fue determinar la improcedencia interpuesta en la vía administrativa en razón de que el derecho de acceso previsto en la Ley Orgánica de Protección de Datos consiste en obtener información de los datos personales de base registrados. Es por ello que no ampara el acceso a documentos concretos ya que dichos documentos pueden contener información relativa a terceras personas.[28]

---

[27] Resoluciones de Tutela de Derechos emitidos por la Agencia Española de Protección de Datos [En línea]. España. Agencia Española de Protección de Datos. Fecha de consulta 14 de Mayo de 2013. [En línea]. Disponible en http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2013/common/pdfs/TD-02152-2012_Resolucion-de-fecha-20-02-2013_Art-ii-culo-15-LOPD.pdf

[28] Resoluciones de Tutela de Derechos emitidos por la Agencia Española de Protección de Datos [En línea]. España. Agencia Española de Protección de Datos. Fecha de consulta 14 de Mayo de 2013. [En línea]. Disponible en http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2011/common/pdfs/TD-00097-2011_Resolucion-de-fecha-07-03-2011_Art-ii-culo-15-LOPD.pdf

Asimismo cabe hacer referencia también a la resolución R/01145/2011 emitida por la Agencia Española de Protección de Datos Personales con respecto de la tutela de derechos de acceso a información personal en el sentido que el sujeto obligado manifiesta no tener conocimiento de la solicitud del reclamante. No obstante, el titular del derecho acredita una relación de servicios específicamente de carácter financiero con el sujeto obligado y en razón de ello se estima que es procedente la solicitud de acceso del reclamante. Por lo que en caso de no hacerlo así se incurriría en una infracción de carácter administrativo.[29]

1.2.2. Derecho de rectificación

El derecho de rectificación[30] es la facultad que otorga la disposición normativa que otorga al afectado para que conmine al responsable del tratamiento de los datos a que cumpla con su obligación de mantener la exactitud de los datos.[31]

El derecho de rectificación es definido en palabras de Belen Veleiro como el derecho que tiene el interesado a que se modifiquen los datos personales que resulten ser inexactos o incompletos.[32]

Los derechos de rectificación son de carácter personalísimos y conceden al titular la posibilidad de exigir al responsable del tratamiento de los datos a la observancia del principio de calidad en el tratamiento. Siendo que, establece como postulado esencial la exactitud y actualización de los datos que sean necesarios para el estricto cumplimiento de las finalidades para las que sean tratados. Este derecho se puede ejercer cuando

[29] Resoluciones de Tutela de Derechos emitidos por la Agencia Española de Protección de Datos [En línea]. España. Agencia Española de Protección de Datos. Fecha de consulta 08 de Mayo de 2013. [En línea]. Disponible en la siguiente página electrónica: http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/index-ides-idphp.php

[30] Cabe hacer la aclaración que en países como España existe la Ley Orgánica 2/1984 de 26 de Marzo, la cual regula el derecho de rectificación en materia informativa , esta ley tiene como objeto principal el derecho que le asiste a toda persona física o a sus herederos, así como a personas morales de rectificar la información difundida por cualquier medio de comunicación social de ciertos hechos que le conciernen y que considera que son inexactos y cuya divulgación puede causarle algún tipo de perjuicio. Este derecho es considerado como una garantía institucional del derecho de los ciudadanos a formar libremente su opinión sobre la base de informaciones verdaderas.

[31] TASCÓN Rodrigo. Ref. 08. 97 p.

[32] VELEIRO Belén. Ref. 15. 94 p.

particularmente los datos recabados han dejado de ser necesarios para la finalidad bajo la cual inicialmente se pretendían registrar, ello en relación con el ámbito y las finalidades legitimas en las que fueron recabados.[33]

Para entender la importancia que reviste este derecho podemos mencionar la sentencia del Tribunal Europeo de Derechos Humanos del 11 de Julio de 2002. Específicamente sobre el caso Christine Goodwin contra el Reino Unido en donde el Tribunal de Estrasburgo declara el derecho a la modificación de ciertos datos registrales de los transexuales en el entendimiento de que el reconocimiento jurídico de los cambios de sexo pueden tener repercusión de la filiación, matrimonio, protección a la vida privada y otros ámbitos del derecho en relación directa con la rectificación a sus datos personales[34] de tal manera que el derecho de rectificación está ligado a:

> *"El derecho de cada uno a establecer los detalles de su identidad como ser humano"*[35]

1.2.2.1. Procedimiento para el ejercicio del derecho de rectificación

Atendiendo a la naturaleza de la exactitud de los datos por parte del responsable de su tratamiento el derecho de rectificación se caracteriza por:

1.- Permitir la corrección de errores, modificar los datos que resulten inexactos o incompletos y garantizar la certeza de la información objeto de tratamiento.

2.-La solicitud de rectificación deberá indicar a que datos se refiere y la corrección que haya de realizarse, de acuerdo a lo establecido en el aviso de privacidad, debiendo en todo

---

[33] CASTAÑEDA, Alberto y BONADEO Rodrigo. Ref. 12. 149 p.

[34] En esta sentencia el Tribunal de Estrasburgo no considera que la rectificación de la condición de transexuales en ciertos registros puede causar dificultades concretas importantes o un ataque al interés público. En todo caso y frente a los inconvenientes que pudieran generarse las modificaciones a sus datos, se considera que se puede razonablemente exigir de la sociedad que acepte aquellos inconvenientes con el fin de permitir a otros vivir con dignidad y respeto conforme a la identidad sexual escogida por ellos en confronta con los enorme sufrimientos que pueden llegar a presentar.

[35] Sentencia del Tribunal Europeo de Derechos Humanos en el asunto Chirstine Goodwim contra Reino Unido de 11 de Julio de 2002.

momento acompañar la documentación justificativa de lo solicitado; sin embargo cabe considerar que el presente derecho es independiente, es decir no se tiene que ejercitar el derecho de acceso o cancelación para solicitarlo. Cabe hacer mención que podrán utilizarse formatos, medios electrónicos, medios remotos u otros que se consideren pertinentes.

3.- Se debe considerar en todo momento la gratuidad en el trámite del ejercicio de este derecho.

Es de considerar que si la información proporcionada en la solicitud ante el responsable del tratamiento de los datos sea insuficiente o errónea para atenderla, o bien, no se acompañen los documentos en donde se acredite la personalidad, señale domicilio para recibir notificaciones y los documentos que justifiquen su petición en el que se señale las modificaciones a realizarse; el responsable podrá requerir al titular, por una vez y dentro de los cinco días siguientes a la recepción de la solicitud, que aporte los elementos o documentos necesarios para dar trámite a la misma. El interesado tendrá diez días hábiles para atender el requerimiento, contados a partir del día hábil siguiente en que le fue notificado. De no dar respuesta en dicho plazo, se tendrá por no presentada la solicitud correspondiente.

4.-El responsable de los datos resolverá sobre la solicitud de rectificación o cancelación en un plazo máximo de 20 días hábiles contados a partir de la recepción de la solicitud.

5.- Si resulta procedente la solicitud de rectificación, se podrá hacer efectiva dentro de los quince días hábiles, posteriores a la fecha en que se comunica la respuesta al interesado.

6.- Cuando el interesado hubiere solicitado del responsable del tratamiento la confirmación de la rectificación del tratamiento de sus datos , éste deberá responder expresamente a su solicitud.

7.-Ahora bien si los datos rectificados hubieran sido cedidos previamente, el responsable del tratamiento de los datos deberá comunicar la rectificación efectuada al cesionario, para efecto de que proceda la rectificación de los mismos.

8.- En caso de que exista una negativa por parte el responsable del tratamiento de los datos ya sea total o parcial, el responsable deberá informar el motivo de su decisión y comunicarla al titular, o en su caso, al representante legal, en los plazos establecidos para tal efecto, por el mismo medio por el que se llevó a cabo la solicitud, acompañando en su caso las pruebas que resulten pertinentes.[36]

Es de considerar que, en caso de que sea imposible la rectificación de los datos, el responsable del tratamiento de los mismos, deberá de cancelar de oficio los datos tratados ello por no ser actualizados ni responder a la situación real del interesado. Por lo tanto conlleva la ilegitimidad en el tratamiento de los datos o en su momento pueden ser disociados a efecto de que los datos se conviertan en anónimos.[37]

1.2.2.2. Causales de denegación al derecho de rectificación

Existen justificaciones legítimas por parte del sujeto regulado para negar la petición del titular de los datos en cuanto al ejercicio del derecho de rectificación, mismos que se detallan a continuación:

1.- Cuando el representante no sea el titular de los datos personales a rectificar, o el representante legal no esté debidamente acreditado para ello; conforme a lo dispuesto en el artículo 89 del Reglamento de la LFDPPP.

2.- Cuando exista un impedimento legal, o la resolución de una autoridad competente que no permita la rectificación de los datos.

---

[36] Agencia Española de Protección de Datos. El derecho fundamental a la protección de datos: Guía para el ciudadano. [En línea]. España 2011. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_CIUDADANO_OK.pdf. 25p.

[37] COUDERT Fanny. Ref. 24. 371 p.

3.-Cuando el interesado no indique de manera precisa los datos que se deben rectificar y los cuáles sean objeto de tratamiento por parte del responsable.

1.2.2.3. Resoluciones relevantes en materia de derecho de rectificación

Cabe hacer mención que dentro del ejercicio de derechos por parte de los titulares de los datos el derecho de rectificación es el menos recurrido, ello en razón de que su fuente derivada de la existencia de un error o inexactitud de los datos. Lo anterior, lo podemos corroborar con la siguiente ilustración en el que se refleja los temas respecto del ejercicio de la tutela efectiva de los derechos ARCO por parte de la Agencia Española de Protección de Datos en el 2011.

TEMAS	%
1. Acceso	15,71%
2. Cancelación	50,35%
3. Rectificación	3,57%
4. Oposición	27,85%
5. Información	2,89%
6. Exclusión de guías	2,50%

Fuente[38]

Resolución Nº.: R/00004/2012

Es esta resolución el interesado ejerce su derecho de rectificación ante la empresa de telefonía celular denominada VODAFONE España S.A.; en dicho documento se hace referencia a la petición de rectificación de datos, sin embargo no se tiene respuesta alguna por parte del responsable del tratamiento de los datos. Por lo tanto el interesado presenta formalmente una solicitud ante la Agencia de Protección de Datos; sin embargo al momento de desarrollarse el procedimiento aludido el sujeto obligado cumple de forma

[38] Memoria de la Agencia Española de Protección de Datos. España. 2011. 90 p.

voluntaria la solicitud de rectificación, por lo que la autoridad declara procedente la reclamación formulada por el titular de los datos.[39]

1.2.3. Derecho de cancelación

Ahora bien otro derecho de suma importancia es el derecho de cancelación por parte del interesado es una de las acciones ponderantes que en su mayoría tramitan los sujetos obligados en cuanto a la tutela efectiva en el ejercicio de los derechos ARCO. Tal situación la podemos corroborar en las estadísticas reflejadas en el 2011 en la consulta sobre ejercicio de derechos de la Agencia Española de Protección de Datos, siendo el derecho de cancelación el más accionado por los interesados con un 51%.[40]

Es importante tener presente que es el derecho de cancelación mismo que es definido por Daniel Santos como:

> "*… la facultad que tiene el afectado para solicitar al responsable del fichero para que cumpla con su obligación de cancelar los datos inexactos, incompletos, inadecuados excesivos, es decir, los datos erróneos que contravengan el principio de veracidad.*"[41]

Sin embargo y para efectos de una mayor compresión del presente ejercicio podemos mencionar también lo que es especie señala Velázquez Bautista, el cual menciona que el derecho de cancelación se entiende como la acción de anular, borrar, hacer ilegible, destruir, dejar irreconocible o declarar nulos los datos del interesado, no obstante cabe señalar que mientras para una legislación de protección de datos equivaldría a destruirlos o borrarlos, para otra legislación esta acción consiste en efectuar un asiento similar al que realizan los registradores de la propiedad en los libros de registro, es decir se declara nula una anotación o se realiza una inscripción marginal de tipo preventivo y por consecuencia los efectos que puede llegar a tener. Bajo este contexto se "declaran nulos" o se "anulan"

---

[39] Resoluciones de Tutela de Derechos emitidos por la Agencia Española de Protección de Datos. España. Agencia Española de Protección de Datos. Fecha de consulta 30 de Mayo de 2013. [En línea]. Disponible en:http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2012/common/pdfs/TD-01846-2011_Resolucion-de-fecha-10-01-2012_Art-ii-culo-16-LOPD.pdf

[40] Memoria de la Agencia Española de Protección de Datos. España. 2011. 90 p

[41] SANTOS Daniel. Nociones generales de la Ley Orgánica de Protección de Datos. Madrid. Editorial Tecnos 2005. 98 p.

los datos personales, pero no se procede a su borrado o a su destrucción, es decir queda constancia fehaciente de que los mismos se han cancelado.[42]

En otro orden de ideas y bajo la perspectiva de Aparicio Salom el derecho de cancelación implica que el interesado solicite la exclusión del tratamiento de los datos de carácter personal, ya sea porque estos presentan un error, o por no interesarle a que se sometan a tratamiento determinado. Cabe aclarar que este derecho puede referirse a la totalidad de los datos o alguno de ellos de manera concreta, por lo que en definitiva el ejercicio del derecho de cancelación puede suponer la terminación de una relación jurídica con el responsable del tratamiento de los datos por voluntad unilateral del interesado.[43]

Para efectos de una compresión consensada del derecho de cancelación, este es entendido de la siguiente manera:

> *"Es el derecho del afectado a que se bloqueen o supriman los datos que resulten ser inadecuados o excesivos, sin perjuicio del deber de bloqueo de datos.[44]"*

Es importante hacer una breve reflexión para una mayor compresión de este derecho lo que en especie dispone la legislación española en cuanto el contenido de la cancelación de datos, destacando la excepción de datos referentes a información de tipo histórico, estadístico y científico que se encuentre en determinados datos de carácter personal específicamente el artículo 4.5 de la Ley Orgánica 15/1999 de 13 de Diciembre. Estas consideraciones no se encuentran previstas en la LFPDPPP y su reglamento es por ello que cabe hacer mención lo que en especie señala el citado artículo el cual textualmente dispone lo siguiente:

> *"Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.*

[42] VELAZQUEZ Rafael. Protección jurídica de datos personales automatizados. Madrid. Colex. 1993. 132 y 133 p.

[43] APARICIO Javier. Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal. Navarra. Editorial Aranzandi. 2000. 139 p.

[44] VELEIRO Belén. Ref. 15. 2008.95 p.

No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados. Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos."

Ahora bien es conveniente puntualizar que la finalidad del derecho de cancelación de acuerdo al criterio de Serrano Pérez es:

"(…) evitar que los datos almacenados se perpetúen y se conviertan en etiquetas definitivas para el individuo, con el peligro que estos supondrían para la identidad y los derechos de las persona. (Piénsese en el lastre que supondría arrastrar durante toda la vida de una persona datos reveladores de conductas antisociales, o en general que implicaran una carga negativa, como tratamientos psiquiátricos, referencias económicas desfavorables, etc. Esta situación se agravaría además si se tratara de referencias a situaciones pasadas y totalmente superadas"[45]

1.2.3.1 Procedimiento para ejercicio del derecho de cancelación

La LFPDPPP establece en su artículo 25 el derecho subjetivo el cual faculta al titular de los datos personales para efectos de que se cancelen lo mismo. Adicionalmente el artículo 10 del Reglamento de la citada dispone que la cancelación atienda a que el titular considera que sus datos personales no están siendo tratados conforme a los principios y deberes que establece la normatividad que los regula.

El derecho de cancelación puede ser ejercido por el titular del derecho o por su represéntate legal en los términos en los que se ha expuesto en la parte general del presente capítulo ante el responsable del tratamiento de los datos atiendo a las siguientes etapas:

[45] SERRANO Pérez en FRUTOS Omar. *El derecho de cancelación de datos personales en archivos privados en México y España*. DERECOM. No 13. Nueva Época. Marzo-Mayo, 2013. 16 p. [En línea]. Consultada el 15 de Mayo de 2013 en http://www.derecom.com/numeros/pdf/frutos.pdf.

1.- El interesado deberá de presentar una solicitud de cancelación de datos en la que deberá plasmarse el nombre y domicilio del titular, o algún otro medio para comunicarle la respuesta a su solicitud, los documentos que acrediten su identidad o la representación legal del titular, la descripción clara y precisa del dato personal que pretende cancelar, así como cualquier otro documento que facilite la localización del dato a cancelar.

2.- Posteriormente el responsable comunicará en un plazo de veinte días hábiles contados a partir de la recepción de la solicitud de cancelación sobre la determinación adoptada, y en caso de ser procedente se haga efectiva dentro de los quince días hábiles siguientes a la fecha de notificación de la respuesta.

3.- La solicitud de cancelación se deberá indicar si el titular de los datos personales revoca el consentimiento otorgado y en su caso acompañar la documentación que lo justifique.

4.- Cabe señalar que en caso de resultar procedente la cancelación de los datos personales se divide en dos facetas:

A).-Bloqueo: Esta operación implica separar los datos del resto o manipularlos de tal manera que se impida su ulterior tratamiento o utilización[46].

B).-Supresión: Una vez que es transcurrido el periodo de bloqueo el responsable del tratamiento de los datos procederá a la destrucción física de los datos cancelados.[47]

Se considera que el periodo de bloqueo será equivalente al periodo de prescripción de las acciones derivadas de la relación jurídica o contractual que funda el tratamiento en los

[46] Cabe señalar que la cancelación no supone automáticamente en todo caso un borrado o supresión físico de los datos, sino que puede determinar, en caso de que así lo establezca una norma con rango de Ley o se desprenda de la propia relación jurídica que vincula al responsable de los datos con el afectado (y que motiva el propio tratamiento), el bloqueo de los datos sometidos a tratamiento.

[47] Davara Rodríguez manifiesta que con el concepto de bloqueo se abre un tema de gran interés centrado en la auditoría informática y la llamada auditoría jurídica. Las diferencias entre supresión y borrado, y entre cancelación y bloqueo, se pueden prestar a múltiples interpretaciones y necesitarían un desarrollo independiente respecto a las medidas de seguridad física y lógica a adoptar para ofrecer la necesaria seguridad jurídica.

términos de la Ley aplicable en la materia, de acuerdo a lo dispuesto en el artículo 107 Fracción I del Reglamento de la LFPDPPP.

Para el caso que se genere el bloqueo de los datos, el responsable del tratamiento estará obligado a conservar los datos en condiciones que aseguren y garanticen el derecho del afectado a la protección de datos de carácter personal. Estas garantías consisten en la restricción al acceso a los mismos, a las personas debidamente designadas en el documento de seguridad siempre que sean mínimas e imprescindibles para la conservación de los datos y en la implantación de medidas de seguridad.[48] Conforme a lo dispuesto en el artículo 107 Fracción III del Reglamento de la LFPDPPP, el bloqueo se llevará a cabo en los 15 días hábiles después de haber notificado al interesado la procedencia de la cancelación de los datos.

Cuando se procede al bloqueo de los datos y no se procede a su borrado físico, el responsable del tratamiento debe justificar que de acuerdo a una disposición legal, o bien la naturaleza jurídica que le vincula al afectado, legitiman el bloqueo, al poder ser requerido por responsabilidades nacidas del tratamiento, siempre y cuando los datos bloqueados sean necesarios para atender dichas responsabilidades.[49]

El bloqueo de los datos se producirá en los casos en que sea posible su extinción física, por razones técnicas o por razones de que el soporte o procedimiento que se utilice impida la cancelación. Si el responsable del tratamiento de la información hubiere recabado los datos por medios fraudulentos o ilegales, su cancelación supondrá además la destrucción del soporte en el que los datos figuren.[50]

[48] COUDERT Fanny. Ref. 24. 373 p.
[49] Ibídem. 374 y 375 p.
[50] SANTOS Daniel. Ref. 41. 99 p.

Es de considerar que los datos de carácter personal bloqueados constituyen un medio de prueba a disposición de las Administraciones Públicas, jueces y tribunales en el ejercicio de sus funciones con las finalidad de acreditar determinados hechos.[51]

5.- En caso de que los datos cancelados han sido comunicados a terceros previamente, el responsable del tratamiento tiene la obligación de notificar la cancelación efectuada a dichos terceros, quienes a su vez proceden a la cancelación de los datos.

El derecho de cancelación de los datos comporta la finalización de la relación jurídica entre el responsable del tratamiento de los datos y el titular de los datos personales que se cancelan.[52]

1.2.3.2 Causales de negativa ante el ejercicio de cancelación de datos personales

Pueden existir supuestos procesales bajo los cuales el responsable del tratamiento de los datos podrá negar la cancelación de los datos personales siempre y cuando concurran las siguientes circunstancias, ello de acuerdo a lo dispuesto en el artículo 34 de la LFPDPPP, los cuales se señalan a continuación:

A).- Cuando el solicitante no sea el titular de los datos personales, o el representante legal no esté debidamente acreditado para ello.

B).-Cuando en su base de datos, no se encuentren los datos personales a cancelar por parte del solicitante.

C).- Cuando se lesionen los derechos de un tercero.

D).-Cuando exista un impedimento legal, o la resolución de una autoridad competente, que no permita la cancelación de los mismos.

E).-Cuando la cancelación haya sido previamente realizada.

[51] COUDERT Fanny. Ref. 24. 374 p.
[52] SANTOS Daniel. Ref. 41. 99 p.

1.2.3.3. Excepciones al derecho de cancelación de datos

El responsable del tratamiento de los datos no siempre está obligado a realizar la cancelación de los datos del interesado, ya que puede presentar algunos supuestos que la LFPDPPP le excluye legalmente el hecho de que sean cancelados, ello conforme a lo dispuesto en el artículo 26 del citado ordenamiento, mismo que a la letra señala lo siguiente:

> *"Artículo 26.- El responsable no estará obligado a cancelar los datos personales cuando:*
>
> *I. Se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento;*
>
> *II. Deban ser tratados por disposición legal;*
>
> *III. Obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas;*
>
> *IV. Sean necesarios para proteger los intereses jurídicamente tutelados del titular;*
>
> *V. Sean necesarios para realizar una acción en función del interés público;*
>
> *VI. Sean necesarios para cumplir con una obligación legalmente adquirida por el titular, y*
>
> *VII. Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto."*

1.2.3.4. Divergencia entre el derecho de cancelación y la revocación del consentimiento

La diferencia esencial entre el derecho de cancelación y revocación del consentimiento consiste en que en la primera de ellas es un derecho subjetivo el cual está sujeto a un contenido determinado el cual deberá de acompañarse de la documentación acreditativa para su ejercicio; y para el segundo se requiere una causa justificada para ello , sin que

se le atribuyan efectos retroactivos.[53] Cabe hacer la aclaración que la cancelación de los datos puede generarse por que se ha podido realizar sin el consentimiento previo del titular del derecho y por lo tanto el afectado decide oponerse al tratamiento de datos. Por lo antes expuesto la cancelación puede ser solicitada por que el titular de los datos ha decidido revocar el consentimiento otorgado al momento en que se recaban los datos.

1.2.3.5. Resoluciones destacadas respecto del derecho de cancelación

Cabe hacer notar las resoluciones referidas a reclamaciones presentadas por la denegación al derecho de cancelación de datos personales obrantes en el Libro de Registros de Bautismos, ya que el criterio de la Agencia Española de Protección de Datos establece lo siguiente:

> *"Registro Bautismal contiene actas de notoriedad, que hacen referencia al hecho histórico del bautismo de una persona sin que se identifique a la misma como miembro de la Iglesia Católica, por lo que no procede la cancelación de sus asientos.*
>
> *En definitiva la Iglesia Católica no posee ficheros de sus miembros, ni relación alguna de ellos, puesto que el asiento del registro bautismal no es identificable con la pertenencia a la Iglesia Católica.*
>
> *No obstante lo anterior, debe hacerse notar que, al tenor del artículo 4.3 de la LOPD, los datos de carácter personal deben responder con veracidad a la situación actual del afectado, por lo que debe reflejarse , mediante anotación marginal en la partida de bautismo del reclamante , del ejercicio del derecho de cancelación".*[54]

Es de especial pronunciamiento la sentencia emitida por la Agencia Española de Protección de Datos emitida el siete de Marzo de 2011; respecto de la resolución número R/00355/2011 la cual resulta sumamente interesante, ello en razón de que el titular de los datos personales solicita concretamente a la autoridad administrativa la eliminación de sus datos que aparecen en Internet mediante la herramienta de búsqueda de Google[55] ya

---

53 DEL PESO Emilio, Ref. 07. 124 p.

54 Ibídem. 128 p.

55 El motor de búsqueda de GOOGLE es un complejo sistema informático que indexa documentos almacenados en millones de servidores de páginas web (más comúnmente conocidos como servidores web), facilitando al usuario del servicio de búsqueda su inmediata localización, a través de determinadas palabras contenidas en los documentos buscados. El índice del motor de búsqueda de GOOGLE se actualiza de forma dinámica a partir de la información obtenida por robots, que continuamente rastrean los servidores web públicamente disponibles en Internet, utilizando para ello la capacidad tecnológica de los propios servidores de la compañía, usualmente conocidos como "arañas web" o "web crawlers". Las "arañas web" analizan de forma metódica páginas web HTML disponibles públicamente, recopilando los hiperenlaces que figuran en éstas (referencias a otras direcciones URL), para extender así su labor de rastreo, de forma encadenada, a todas las páginas y documentos referenciados. El rastreo consiste en extraer, de todos los documentos

que este servicio utiliza tratamiento de datos personales. Este documento establece en su parte resolutiva la declaración de procedencia respecto de la reclamación formulada por el interesado ordenando la cancelación de los datos personales del interesado. Se considero especialmente lo dispuesto en el resolutivo TD/266/2007 para solucionar dicho expediente, mismo que en esencia señala lo siguiente:

> *"Por todo ello, cabe proclamar que ningún ciudadano que ni goce de la condición de personaje público ni sea objeto de hecho noticiable de relevancia pública tiene que resignarse a soportar que sus datos de carácter personal circulen por la RED sin poder reaccionar ni corregir la inclusión ilegitima de los mismos en un sistema de comunicación universal como Internet. Si requerir el consentimiento individualizado de los ciudadanos para incluir sus datos personales en Internet o exigir mecanismos técnicos que impidieran o filtraran la incorporación inconsentida de datos personales podría suponer una insoportable barrera al libre ejercicio de las libertades de expresión e información a modo de censura previa (lo que resulta constitucionalmente proscrito), no es menos cierto que resulta palmariamente legítimo que el ciudadano que no esté obligado a someterse a la disciplina del ejercicio de las referidas libertas (por no resultar sus datos personales de interés público y contribuir, en consecuencia, su conocimiento a forjar una opinión pública libre como pilar basilar del Estado democrático) debe gozar de mecanismos reactivos amparados en Derecho (como el derecho de cancelación de datos de carácter personal) que impidan el mantenimiento secular y universal en la Red de su información de carácter personal"*[56]

Otro criterio relevante es aquel emitido por el Tribunal Europeo de Derechos Humanos respecto a la negativa de un sujeto obligado derivado de la solicitud de cancelación de datos personales concernientes a las actividades profesionales mismas que a la letra señala lo siguiente:

> "*A este respecto es irrelevante el hecho de que los datos publicados se refieran a actividades profesionales (véase la sentencia Osterreichischer Rundfunk y otros*[57]*, antes citada, apartados 73 y*

visitados (no sólo de las páginas con formato HTML, sino también de los documentos que presentan otros formatos), las palabras clave que serán indexadas.

56 Resoluciones de Tutela de Derechos emitidos por la Agencia Española de Protección de Datos [En línea]. España. Agencia Española de Protección de Datos. Fecha de consulta 14 de Mayo de 2013. [En línea]. Disponible en http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2011/common/pdfs/TD-01075-2010_Resolucion-de-fecha-07-03-2011_Art-ii-culo-16-LOPD_Recurrida.pdf

57 Los artículos 6, apartado 1, letra c), y 7, letras c) y e), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, no se oponen a una normativa nacional, como la controvertida en los asuntos principales, siempre que se demuestre que la amplia divulgación no sólo del I - 5051 SENTENCIA DE 20.5.2003 — ASUNTOS ACUMULADOS C-465/00, C-138/01 Y C-139/01 importe de los ingresos anuales, cuando éstos superan un límite determinado, de las personas empleadas por

74). El tribunal Europeo de Derechos Humanos ha declarado a este respecto que los términos "vida privada" no debían interpretarse restrictivamente y que "ninguna razón de principio permite excluir las actividades profesionales (…) de concepto de vida privada" (véase en particular TEDH, sentencias antes citadas Amann C .Suiza 65. Rotaru C. Rumania 43)" [58]

En lo que respecta a México podemos mencionar la resolución relativa al expediente PPD. 0002/2012, en la que se promueve por parte del titular su derecho de cancelación frente a Banco Azteca S.A. Institución de Banca múltiple, específicamente en lo que respecta a la cancelación y retiro de una fotografía digital, contenida en la base de datos de la responsable del tratamiento ello en razón de que en ningún momento se solicito autorización de la titular y no se otorgo consentimiento expreso. En consecuencia el Instituto Federal de Acceso a la Información y Protección de Datos resuelve ordenar la cancelación de los datos del accionante.[59]

1.2.4. Derecho de oposición

El derecho de oposición es una facultad en la que se reconoce al interesado la potestad de oponerse al tratamiento de sus datos de carácter personal en aquellos supuestos en que no sea preciso recabar su consentimiento siempre que la ley no disponga lo contrario.[60] El interesado podrá oponerse al tratamiento de sus datos de carácter personal cuando concurra una razón legítima derivada de su concreta situación personal.[61]

---

entidades sujetas al control del Rechnungshof, sino también de los nombres de los beneficiarios de dichos ingresos, es necesaria y apropiada para lograr el objetivo de buena gestión de los recursos públicos perseguido por el constituyente, extremo que ha de ser comprobado por los órganos jurisdiccionales remitentes.

[58] Resoluciones de Tutela de Derechos emitidos por la Agencia Española de Protección de Datos [En línea]. España. Agencia Española de Protección de Datos. Fecha de consulta 14 de Mayo de 2013. [En línea]. Disponible en http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2011/common/pdfs/TD-01248-2011_Resolucion-de-fecha-30-12-2011_Art-ii-culo-34-RD-1720-b-2007.pdf

[59] Resoluciones de Tutela de Derechos emitidos por la Instituto Federal de Acceso a la Información y Protección de Datos [En línea]. México. Fecha de consulta 01 de Junio de 2013. [En línea].Disponible en http://consultas.ifai.org.mx/SesionesspDPTema?tema=14&subtema=2

[60] VELEIRO Belén. Ref. 15. 96 p.

[61] Estándares Internacionales sobre Protección de Datos Personales y Privacidad. Resolución de Madrid. Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad en relación con el tratamiento de Datos de Carácter Personal. Conferencia Internacional de Autoridades de Protección de Datos y Privacidad 5 de Noviembre de 2009.

El derecho de oposición juega en relación a los datos personales para cuyo tratamiento no es necesario el consentimiento del interesado. De igual forma que lo hace la revocación del consentimiento de aquellos datos para los que sí exige éste, si bien, y a diferencia de la revocación, el derecho de oposición debe ser motivado en una concreta situación personal.[62] Este derecho legitima al interesado para que en los casos en que no se necesite el consentimiento del titular de los datos. En consecuencia podrá oponerse al tratamiento de los mismos siempre que existan motivos fundados y legítimos.[63]

Los derechos de oposición a las decisiones basadas únicamente en un tratamiento automatizado de datos, pueden ser impugnadas por el interesados ya que estos tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre de ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de sus personalidad tales como su rendimiento laboral, crédito, fiabilidad o conducta.[64]

En el ejercicio de derecho de oposición se deberá comprobar la existencia de un motivo fundado y legitimo relativo a una concreta situación personal en la que proceda. Posteriormente se deberá de indicar al interesado si se acepta o se niega su solicitud y adoptar las medidas oportunas que pueden consistir en abstenerse de realizar determinada conducta o en cancelar los datos de los cuales se acude a su petición.[65]

En el caso de los datos obtenidos de fuentes accesibles al público el titular de los datos personales tendrá derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que le conciernan, en cuyo caso serán dados de baja del tratamiento. Por lo que en

---

[62] TELLEZ Abel. Ref. 09. 163 p.

[63] CASTAÑEDA, Alberto y BONADEO Rodrigo. Ref. 12. 150 p.

[64] SALLA Xavi y ORTEGA Jorge. *Actuaciones inspectoras en materia de protección de datos.* España. Bosch Editor. 2008. 139 p.

[65] COUDERT Fanny. Ref. 24. 375 p.

consecuencia se cancelan las informaciones que sobre él figuren en aquél, a su simple solicitud.[66]

El Parlamento Europeo ha señalado que el derecho de oposición debe poder ejercerse en cualquier momento y, en particular, frente a los tratamientos con fines de prospección ya sea una prospección comercial o la que efectué un organismo de caridad o un partido político.[67]

El interesado podrá oponerse al tratamiento de sus datos de carácter personal o se cese en el mismo cuando se actualicen los siguientes supuestos:[68]

1.- Cuando no sea necesario su consentimiento para el tratamiento, como consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal.

2.-Cuando se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial.

3.-Cuando el tratamiento tenga como finalidad la adopción de una decisión referida al afectado y se encuentre basada únicamente en un tratamiento automatizado de sus datos de carácter personal; considerando que no debe de existir una afectación de manera significativa.

4.-Se haya celebrado o ejecutado un contrato a petición del interesado, siempre que se le otorgue la posibilidad de alegar lo que estimará pertinente a fin de defender su derecho o interés.

---

66 Guía del Responsable de Ficheros. Agencia Española de Protección de Datos. España. 29 p.

67 CONDE Concepción. *La protección de datos personales*. España. Editorial Dykinson S.L. 2005. 88 p.

68 VELEIRO Belén. Ref. 15. 96 y 97 p.

5.- Se encuentre autorizada por una norma con rango de ley que establezca medidas que garanticen el interés legítimo del interesado.

Es importante señalar que cuando se ejerce el derecho de oposición y procede la cancelación de los datos se puede proceder al bloqueo si es necesario para atender posibles responsabilidades nacidas del tratamiento de los datos.[69]

1.2.4.1. Procedimiento para ejercitar el derecho de oposición

1.- El interesado o su representante legal podrán solicitar al responsable del tratamiento de los datos la oposición de los datos que le conciernen.

2.- La solicitud para ejercer el derecho de oposición deberá contener en términos del artículo 29 de la LFPDPPP: el nombre del titular y domicilio u otro medio para comunicarle la respuesta a su solicitud; los documentos que acrediten la identidad o, en su caso, la representación legal del titular; la descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados y, cualquier otro elemento o documento que facilite la localización de los datos personales.

3.- El responsable comunicará al titular, en un plazo máximo de veinte días hábiles, contados a partir de la fecha en que se recibió la solicitud de oposición, la determinación adoptada, a efecto de que, si resulta procedente, se haga efectiva la misma dentro de los quince días hábiles siguientes a la fecha en que se comunica la respuesta.

1.2.4.2. Causales de negativa al derecho de oposición

En términos del artículo 34 de la LFPDPPP el responsable podrá negar el acceso a los datos personales, o a realizar la rectificación o cancelación o conceder la oposición al

[69] COUDERT Fanny. Ref 24. 375 p.

tratamiento de los mismos, cuando concurran alguna de las siguientes circunstancias: En el caso que la oposición haya sido previamente realizada y cuando el solicitante no sea el titular de los datos personales o el representante legal no esté debidamente acreditado para ello. Cuando en su base de datos no obren los datos personales a los que el solicitante pretende oponerse. Ahora bien para el caso que se lesionen los derechos de un tercero. En caso de existir un impedimento legal o la resolución de una autoridad competente que restrinja la oposición de los mismos. En atención a este último supuesto del al ejercicio de derecho de oposición podemos señalar una disposición en contrario en la que prevalezca el interés público como lo podemos ejemplificar en la resolución R/00368/2004 emitida por la Agencia Española de Protección de Datos misma que a la letra dice:

> *"En cuanto a los motivos fundados expuestos por el reclamante para justificar su oposición a identificarse en los acuses de recibo de los envíos de entrega bajo firma que saque a reparto durante la jornada de trabajo… hay que señalar que la cumplimentación de los datos … forman parte de las obligaciones como empleado del operador que, por mandato legal tiene encomendada la prestación del servicio postal universal, a fin de poder cumplir con los requerimientos exigidos por la normativa …Concretamente el artículo 41.3 del citado reglamento, establece expresamente la obligación del empleado postal de hacer constar su firma y número de identificación en el aviso de recibo, norma que tiene su correlativo reflejo en el Manual de Procedimientos y Productos de Correos. En consecuencia, en el presente caso existe una norma con rango de ley que expresamente exige lo contrario a lo alegado para fundar el ejercicio del derecho de oposición"*[70]

En los estándares internacionales sobre protección de datos personales y privacidad se mediante la resolución de Madrid, se acordó que no procederá el ejercicio del derecho de oposición en aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación impuesta sobre la persona responsable por la legislación nacional aplicable.[71]

---

70 DEL PESO Emilio, Ref. 07. 133 y 134 p.

71 Estándares Internacionales sobre Protección de Datos Personales y Privacidad. Resolución de Madrid. Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad en relación con el tratamiento de Datos de Carácter Personal .Conferencia Internacional de Autoridades de Protección de Datos y Privacidad 5 de Noviembre de 2009.

1.2.4.3 Listados de exclusión

Puede presentarse la circunstancia que organismos privados realice el tratamiento de los datos se realice con fines de publicidad y prospección de tipo comercial, por lo tanto se le reconoce la posibilidad al titular de los datos personales de ser incluido en los denominados listados Robinson.[72] Para el caso de España o el Registro Público Para Evitar Publicidad (REPEP)[73] así como el Registro Público de usuarios que no desean información publicitaria de productos y servicios financieros (REUS)[74] para el caso de México.

Lo antes expuesto queda manifiesto en el artículo 110 del Reglamento de la LFPDPPP, mismo que señala que para el ejercicio del derecho de oposición, los responsables podrán gestionar listados de exclusión propios en los que incluyan los datos de las personas que han manifestado su negativa para que trate sus datos personales, ya sea para sus productos o de terceras personas. Asimismo, los responsables podrán gestionar listados comunes de exclusión por sectores o generales. En ambos casos, la inscripción del titular a dichos listados deberá ser gratuita y otorgar al titular una constancia de su inscripción al mismo, a través de los mecanismos que el responsable determine.

---

[72] Los listados Robinson es un servicio de exclusión publicitaria a disposición de los consumidores gestionado por la Asociación Española de la Economía Digital, que tiene como objetivo disminuir la publicidad que éstos reciben. El Servicio de Listas Robinson se enmarca en el ámbito de la publicidad personalizada, es decir, aquella publicidad que recibe un usuario a su nombre y dirección. Este tipo de publicidad en la actualidad es una actividad necesaria desarrollada por todo tipo de entidades ya sean privadas o públicas, con ánimo de lucro o no. La relevancia que para el avance y progreso de la actividad económica, social o cultural desarrollada por cualquier tipo de entidad, ya sea privada o pública, con ánimo de lucro o no, tiene el tratamiento de datos de carácter personal en general, y los realizados con fines publicitarios, en particular, es una realidad reconocida en la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[73] El 4 de febrero de 2004, se publicó en el Diario Oficial de la Federación el Decreto por el que se reformó y adicionó la Ley Federal de Protección al Consumidor estableciendo el REPEP siendo este un mecanismo de protección que sirve para facilitar el ejercicio del derecho de los consumidores a no ser molestados con publicidad no deseada y a que su información no sea utilizada con fines mercadotécnicos o publicitarios. A pesar de que existen diversos medios a través de los cuales los consumidores pueden recibir publicidad, como parte de una primera etapa se protegerá solo a los consumidores que no deseen ser molestados en su número telefónico.

[74] El REUS es un padrón que contiene información personal de los Usuarios del sistema financiero mexicano que no desean ser molestados con publicidad y promociones por parte de las Instituciones Financieras en sus prácticas de mercadotecnia.

1.2.5. Tratamiento de datos personales en decisiones sin intervención humana valorativa

Es muy común que nuestros datos personales sean considerados como parte de un proceso de toma de decisiones sin que intervenga la valoración de una persona física, por lo que el responsable deberá informar al titular que esta situación ocurre.

Sin embargo, la LFPDPPP no dispone nada al respecto, únicamente en su reglamento encontramos un artículo que hace referencia a esta figura misma que señala textualmente lo siguiente en su párrafo segundo:

> *"Asimismo, el titular podrá ejercer su derecho de acceso, a fin de conocer los datos personales que se utilizaron como parte de la toma de decisión correspondiente y, de ser el caso, el derecho de rectificación, cuando considere que alguno de los datos personales utilizados sea inexacto o incompleto, para que, de acuerdo con los mecanismos que el responsable tenga implementados para tal fin, esté en posibilidad de solicitar la reconsideración de la decisión tomada."*

Es de especial pronunciamiento lo que al respecto señala Guillermo Wolf en su carácter de vicepresidente ejecutivo y director general de la American Chamber/México en su documento intitulado "Comentarios al Anteproyecto del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares" respecto del tratamiento de datos personales en decisiones sin intervención humana valorativa, mismo que a la letra dice:

> *"Se sugiere eliminar este articulo pues se está previendo un derecho para los Titulares no contemplado en la Ley; así como un trámite no previsto en la misma. Debe valorarse que la Ley prevé los derechos ARCO pero en ningún momento establece la posibilidad de que el Titular presente una solicitud ante el Responsable para obtener información relativa a las condiciones y generalidades del tratamiento, así como tampoco establece obligaciones de acceso para la información que generan los responsables para la toma de decisiones en los que no hay intervención humana valorativa. La información generada por los responsables para la toma de decisiones en las que no interviene la*

valoración humana, sino sistemas, no es información del Titular, pues de éste son los datos personales, no así las decisiones de negocio de un responsable".[75]

1.2.5.1. El tratamiento de los datos personales en decisiones sin intervención humana valorativa en España.

En el sistema jurídico español esta figura es conocida como "Derecho de impugnación de valores"; su origen está basado exclusivamente en el tratamiento automatizado de los datos personales por los que se pueda obtener información de la personalidad del interesado.[76] En este derecho el ciudadano puede oponerse a las decisiones con efectos jurídicos sobre él o que le afecten de manera significativa el cual se derive en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.[77]

Desde la perspectiva de Daniel Santos el derecho de impugnación de valores toma como punto de partida la valoración automática de las características y comportamiento de los consumidores a través de diferentes tipos de técnicas informáticas entre ellas el "scoring"[78] no son más que valoraciones automáticas que permiten adecuar los requisitos de una empresa a las necesidad de los consumidores que van a contratar con ella.[79]

Los responsables del tratamiento de los datos que realizan actividades de este tipo, recaban datos del propio interesado o de personas distintas al interesado con la finalidad de valorarlos en conjunto para llegar a definir características personales de cada individuo. Por lo tanto los afectados en todo momento tienen derecho a impugnar las

---

75 Comentarios al Anteproyecto del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Emitido por Guillermo Wolf en su carácter de vicepresidente ejecutivo y director general de la American Chamber/México. México. 2011. [En línea]. Consultado el día 9 de Junio de 2013. Disponible en: http://207.248.177.30/expediente/v99/_B001102856.pdf

76 CASTAÑEDA, Alberto y BONADEO Rodrigo. Ref. 12. 151 p.

77 ENÉRIZ OLAECHEA Francisco Javier y BELTRÁN AGUIRRE Juan Luis. *La protección de los datos de carácter personal*. Pamplona. Institución del Defensor del Pueblo de la Comunidad Floral de Navarra. 2012. 77 p.

78 El "scoring" es considerado como una técnica en el que se asigna puntuación, califica la aptitud crediticia de una persona, ello en base a ciertos criterios ya determinados. Un operador facilita a otra entidad especializada información respecto de la solvencia patrimonial y crédito en relación con sus propios o potenciales clientes. Este proceso sirve para rechazar o no la solicitud de un potencial cliente.

79 SANTOS Daniel. Ref. 41. 92 p.

valoraciones y a la cancelación de los datos después de no ser necesarios para la finalidad para la que fueron recabados. Los afectados tienen incluso derecho a la rectificación de los datos que no sean exactos. Los afectados pueden proceder a la impugnación de valores cuando les afecte mediante un escrito dirigido al responsable del tratamiento de los datos, con una petición de información acerca de los criterios de valoración que utiliza y los programas que le sirven para arribar a esas conclusiones.[80]

El derecho de impugnación de valores está condicionado por dos supuestos: Por una parte se requiere que las decisiones adoptadas tengan efectos jurídicos, ello representa que la decisión basadas en el tratamiento de datos debe afectar los derechos fundamentales y las libertades públicas de los interesados. Por otra parte la decisión adoptada debe afectar a los ciudadanos de manera significativa.

Es de considerar que el afectado podrá impugnar cualquier acto administrativo o decisión privada, tenga o no efectos jurídicos y aunque no le afecten de manera significativa además puede obtener información del responsable del tratamiento sobre los criterios de valoración y el programa utilizado en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.[81]

Debemos mencionar también que la valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado. Ahora bien en el supuesto que se pretenda utilizar el resultado de dicho tratamiento de datos por parte de un tercero en un proceso de carácter jurisdiccional o administrativo no tendrá valor alguno.[82]

[80] Ibídem. 93 p.
[81] COUDERT Fanny. Ref. 24. 376 p.
[82] TELLEZ Abel. Ref. 09. 164 p.

La doctrina se ha mostrado escéptica respecto de la eficacia de este derecho ya que por una parte es cierto que los individuos pueden oponerse a este tipo de decisiones. Por otra parte se debe garantizar la existencia de las mismas supone el reconocimiento de que, a través de dichas decisiones se realizan y se realizaran "perfiles informáticos de los individuos"[83] debiendo considerar también que la personalidad de los titulares de datos y sus aptitudes o comportamientos personales. No pueden predeterminarse en un aspecto público o privado mediante el tratamiento de sus datos ya que puede atentar en contra de su honor y de su intimidad.[84]

Conclusión Capitular

En el presente capitulo hemos visto las características principales de los derechos que cualquier ciudadano puede ejercer frente a otro particular que cuenta con sus datos personales. Siendo que estos derechos de acceso, rectificación, cancelación y oposición (ARCO) fueron definidos para una mayor comprensión de los mismos y se establecieron algunas de sus características principales. Adicionalmente se explico a detalle el procedimiento para su ejercicio, así como algunas excepciones que puede justificar la negativa a dichos derechos por parte de los sujetos obligados. Por último se abordaron algunos aspectos relevantes con respecto al pronunciamiento de algunas autoridades en materia de protección de datos personales sobre algunos puntos controvertidos que se suscitaron en el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de datos personales. En otro orden de ideas cabe destacar también el análisis desarrollado en el derecho de cancelación con respecto a la diferencia que existe entre la revocación del consentimiento y el derecho de cancelación.

[83] ARENAS Mónica. El derecho fundamental a la protección de datos personales en Europa. Valencia. Tirant lo Blanch. 2006. 501 p.
[84] CASTAÑEDA, Alberto y BONADEO Rodrigo. Ref. 12. 150 p.

CAPÍTULO SEGUNDO

En el presente capítulo se abordarán las facultades de verificación por parte del IFAI en cuanto a definiciones, los sujetos regulados, casos de procedencia, sujetos que intervienen, elementos formales, requisitos de procedibilidad, medidas de seguridad, notificaciones, procedimiento de verificación, normas procesales, informe final y conclusiones. Adicionalmente se analizan sus consecuencias jurídicas, legislación aplicable y supletoria, atribuciones de la autoridad en materia de verificación y los medios de impugnación que se pueden interponer ante la autoridad competente.

Procedimiento de verificación en materia de protección de datos personales

El procedimiento de verificación en materia de protección de datos personales es un acto administrativo por el cual un organismo independiente designado por el ordenamiento jurídico como garante de la legalidad y del correcto tratamiento de los datos de carácter personal se encarga de realizar acciones de comprobación, supervisión y control a una o varias personas físicas o entes diferenciados con el fin de detectar, documentar y corregir posibles conductas antijurídicas en materia de su competencia por razón de materia y territorio.[85]

2.1. Objeto de la verificación

En el procedimiento de verificación realizado por el IFAI hacia los sujetos regulados tiene los siguientes objetivos principales:

1.- Analizar hechos que pudieran justificar la incoación del procedimiento sancionador.

2.-Identificar a las personas responsables de una probable infracción.

[85] SALLA Xavi y ORTEGA Jorge. Ref. 64. 69 p.

3.- Determinar circunstancias relevantes en el caso que las hubiera para elaborar el informe correspondiente para su corrección.[86]

El IFAI es la autoridad administrativa[87] encargada del ejercicio y vigilancia de las disposiciones en materia de protección de datos personales previstos en la LFPDPPP de acuerdo con lo dispuesto en sus artículos 38, 39 y 59 del citado ordenamiento por ello cuenta con facultades suficientes para realizar las visitas de verificación que correspondan.

2.2. Sujetos que intervienen en el procedimiento de verificación

1.- Instituto Federal de Acceso a la Información y Protección de Datos, en su calidad de autoridad verificadora.

2.- Titular de los datos o su representante legal.

3.- El responsable y en el encargado del tratamiento de los datos.

2.3. Fases del procedimiento de verificación

Para su mejor comprensión y análisis dentro del procedimiento de verificación se pueden establecer 5 fases, mismas que a continuación se explican:

Primera Fase.- Admisión.- El IFAI tienen las facultades de comprobar el cumplimiento de las disposiciones previstas en la LFPDPPP por lo tanto podrá iniciar el

86 HECKH Norman Coordinador. Memento Experto. Protección de Datos. España. Ediciones Francis Lefebvre. 2012. 220 p.

87 Cabe mencionar que en el ejercicio del procedimiento de verificación el personal del instituto tiene fe pública para constatar la veracidad de los hechos en relación con los tramites a su cargo ello con fundamento en lo dispuesto en el artículo 130 de su Reglamento.

procedimiento de verificación conforme a los dispuesto en los artículos 128 y 129 del reglamento mediante las siguientes causales de procedencia:

1.1. Por oficio, es decir por propuesta interna del mismo Instituto.

1.2. Petición del interesado o su representante legal.

1.3. Denuncia

1.4. Instrucción del Pleno del Instituto. En este supuesto el Pleno del IFAI podrá valorar los escritos dirigidos por otros órganos administrativos en los que se comuniquen hechos susceptibles de investigación.

1.5. Planes sectoriales. Consisten en comisionar a un determinado número de verificadores para que realicen una serie de inspecciones en un determinado sector económico (banca, comunicaciones, hoteles y determinar el grado de cumplimiento de las normas aplicables).[88]

Segunda Fase.- Análisis de oportunidad para realizar la verificación

En esta fase es conveniente analizar la documentación presentada por el denunciante, ya que puede presentarse la inexistencia de razones para iniciar un procedimiento administrativo sancionador derivados de los siguientes motivos:

2.1. Cuando se trata de datos referentes a persona morales.

2.2. Cuando se presenten denuncias contra medios de comunicación sobre aspectos relativos a datos publicados en el mismo que puedan afectar el honor o la intimidad, así como la propia imagen.

[88] MARZO Ana. Infracciones y sanciones. En: ALMUZARA Cristina: Estudio práctico sobre la protección de datos de carácter personal. España. Editorial LEX NOVA S.A. 2005. 77-81 p.

2.3 Cuando no se produce el tratamiento de datos de carácter personal derivado de una persona física.

Tercera fase.- Desarrollo de la verificación

Una vez que se ha tenido conocimiento de los hechos presuntamente constitutivos de una infracción en protección de datos personales ya sea por denuncia o a petición de parte se les correrá traslado al sujeto regulado derivado del acuerdo de inicio dictado por el pleno del Instituto, considerando que el plazo para la conclusión del mismo no podrá exceder de 180 días hábiles, pudiendo el pleno ampliar `por una sola vez y hasta por un periodo igual al plazo aludido, ello con fundamento en lo dispuesto en su artículo 132 de su Reglamento.

Es de considerar que se conservarán los documentos obtenidos durante la tramitación de la verificación en un expediente que estará bajo resguardo de la autoridad el cual tendrá el carácter de confidencial.

El IFAI por conducto de su personal debidamente acreditado podrá realizar diversas visitas de verificación mediante una orden escrita debidamente fundada y motivada emitida por la Secretaria de Protección de Datos Personales conforme a lo dispuesto en el artículo 24 Fracción XX del Reglamento Interior del Instituto Federal de Acceso a la Información y Protección de Datos, en ejercicio de las atribuciones conferidas a la Dirección General de Verificación con fundamento en lo dispuesto en el artículo 39 Fracción II del citado ordenamiento de la cual se dejará copia con quien se entendió la visita.

Con objeto de acreditar los hechos que se están investigando, el responsable de llevar a cabo la verificación podrá acceder a diversas fuentes de información que ofrezcan datos sobre los sujetos regulados como puede ser:

-Registros

-Información telefónica
-Publicaciones
-Otro tipo de fuentes accesibles al público
-Examen de soportes de información
-Examen de equipos físicos
-Verificación de programas
-Examinar sistemas de transmisión y acceso de datos
-Auditorías realizadas

Se debe considerar que cuando sea preciso el tratamiento de soportes informáticos en el desarrollo de una investigación, se podrá incorporar diligencias firmadas en la que se hará constar la fecha y el procedimiento seguido para el análisis y a la que se podrán adjuntar los posibles subproductos, siempre que sean relevantes para la investigación.

Cabe señalar que los verificadores actuantes deberán identificarse mediante la exhibición de una credencial vigente con fotografía que los acredite como servidores públicos del Instituto que lo acrediten para desempeñar dicha función; conforme a lo dispuesto en el artículo 134 del Reglamento de la LFPDPPP.

Es conveniente que durante el proceso de verificación siempre que sea posible de los datos personales dejar evidencia de los documentos a que se tengan acceso, cuando estos sean relevantes para el esclarecimiento de los hechos investigados. Por lo que en consecuencia también se obtendrá evidencia clara sobre el tratamiento de los mismos.

Cuarta fase.- Cierre del Acta.

Al concluir la visita de verificación se levantará un acta en la que quedará constancia de las actuaciones practicadas durante la visita o visitas de verificación. Dicha acta será levantada ante la presencia de dos testigos propuestos por la persona con quien se hubiera entendido la diligencia o por quien la practique si aquella se hubiere negado a proponerlos.

La citada acta se emitirá por duplicado la cual será firmada por el personal verificador que actúa en la diligencia, así como el responsable, encargado o con quien se haya realizado la actuación, quien podrá realizar las manifestaciones que a su derecho convenga. Si el sujeto verificado se niega a firmar el acta se dejará constancia de ello en la misma, cabe mencionar que dicha negativa no afecta la validez de las actuaciones o de la propia acta. Es de considerar que la firma del verificado no supone la conformidad respecto del contenido de dicha acta, tan solo acredita la recepción de la misma.

Los elementos formales de las actas de verificación conforme a lo dispuesto en el artículo 136 del Reglamento serán los siguientes:

1.- Nombre, denominación o razón social del verificado.

2.- Hora, día, mes y año en que se inicie y concluya la verificación.

3.- Los datos que identifiquen plenamente el domicilio, como calle, número, población o colonia, municipio o delegación, código postal y la entidad federativa en que se encuentre ubicado el lugar en el que se practique la verificación, así como el número telefónico u alguna otra forma de comunicación disponible con el verificado.

4.-Número y fecha del oficio de comisión que lo motivó.

5.- Número y cargo de la persona con quien se entiende la verificación.

6.-Nombre y domicilio de las personas que fungieron como testigos.

7.- Todos los datos relativos a las actuaciones y hallazgos.

8.- Manifestaciones del verificado o quien se entienda la diligencia en caso de querer realizarlas.

9.- Nombre y firma de quienes intervienen en la verificación, incluyendo a los servidores públicos que la realizaron.

Para el caso de la negativa a firmar por parte del verificado, su representante legal o la persona con quien se entendió la verificación se asentará la razón relativa a ello.

Los verificados a quien se haya levantado acta de verificación adicionalmente podrán hacer las manifestaciones pertinentes dentro del término de cinco días hábiles posteriores a la fecha en que se hubiere levantado el acta correspondiente.

Quinta fase.- Conclusión de las actuaciones de verificación.

Una vez finalizadas las actuaciones y levantada el acta la Dirección General de Verificación emitirá un informe o reporte en el que se incluirá una descripción de los hechos, actuaciones practicadas y conclusiones, dicho expediente será remitido al pleno del Instituto para efectos de que emita una resolución en los siguientes términos:[89]

5.1. Cumplimiento de medidas que deberá adoptar el sujeto regulado, mismo que deberán ser cumplida en un determinado plazo que el mismo instituto señale.

5.2. Inicio del procedimiento de imposición de sanción o establecer un plazo para su inicio. Lo anterior de acuerdo a lo que determine la resolución del Pleno del IFAI, mismo que deberá ser notificada al verificado y, en el caso que proceda al denunciante.

5.3. Archivo del expediente por falta de elementos.

89 LÓPEZ CALVO José. Actividad inspectora y procedimiento administrativo sancionador en materia de protección de datos personales. En: AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. La potestad sancionadora de la Agencia Española de Protección de Datos. España. Editorial Aranzadi. 2008. 256-260 p.

2.4. Elementos sustantivos que pueden ser objeto de análisis en un procedimiento de verificación de datos

En primer término se verificará que los responsables del tratamiento de los datos se apeguen a los principios, de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad de acuerdo a lo establecido en el artículo 6 de la LFPDPPP y artículo 6 de su Reglamento.[90]

Desde la perspectiva de Xavi Salla y Jorge Ortega Soriano se puede establecer una serie de elementos que pueden ser objeto de un proceso de verificación los cuales se mencionarán a continuación:[91]

a).- Medidas de Seguridad

Responsable de la Seguridad de los datos: la cual consiste en que el responsable de los archivos designará a uno o varios responsables de seguridad que coordinarán y controlarán las medidas de seguridad. Ello no supone delegación de la responsabilidad del responsable de la información.

b).-Funciones y obligaciones del personal.

Las funciones y obligaciones de cada una de las personas estarán claramente definidas y documentadas.

---

[90] Dichos principios consisten en lo siguiente: Licitud se obliga al responsable del tratamiento a que cumpla con la legislación mexicana y el derecho internacional. Consentimiento este se deberá recabar para el tratamiento de los datos personales de acurdo a la finalidad de los mismos, el cual deberá ser libre, específico e informado. Calidad nos referimos a aquellos datos personales que sean exactos, completos, pertinentes, correctos y actualizados. La finalidad consiste en que los datos personales solo podrán ser tratados de acuerdo al aviso de privacidad. La lealtad atiende a la obligación de tratar datos personales privilegiando los intereses del titular y la expectativa razonable de privacidad. La proporcionalidad consiste en el tratamiento de los datos cuando resulten necesarios, adecuados y relevantes en relación con la finalidad. Por último el principio de responsabilidad atiende a la obligación del responsable de responder por el tratamiento de los datos personales que se encuentran bajo su custodia.

[91] SALLA Xavi y ORTEGA Jorge. Ref. 64. 87-94 p.

El responsable del archivo adoptará las medidas necesarias para que el personal conozca las normas de seguridad que afectan el desarrollo de sus funciones así como las consecuencias en que pudiere incurrir en caso de incumplimiento.

El responsable del archivo comprobará que todo el personal del encargado del tratamiento de los datos tenga suscrito el correspondiente compromiso de confidencialidad.

c)- Registro de incidencias.[92]

El procedimiento de notificación y gestión de incidencias contendrá el tipo, momento, la persona que notifica, a quien se le comunica y los efectos que se hayan derivado de la misma.

El registro consignará los procedimientos realizados de recuperación de datos, indicando la persona que ejecuto el proceso, los datos restaurados y, en su caso, que datos han sido necesarios grabar manualmente en procesos de recuperación.

Será necesaria la autorización por escrito del responsable del archivo para la ejecución de los procedimientos de recuperación de los datos.

d).-Identificación y autorización

El responsable del archivo se encargará de que exista una relación actualizada de usuarios con acceso autorizado al sistema de información, con procedimientos de identificación y autenticación para dicho acceso.

[92] Se entiende por incidencia a cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos personales.

En caso de autenticación de contraseña, existirá un procedimiento de asignación, distribución y almacenamiento será de forma ininteligible mientras estén vigentes.

El responsable del archivo establecerá un mecanismo que permita la identidad de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

e).-Control de acceso

Los usuarios sólo tendrán acceso autorizado a datos y recursos necesarios para sus funciones.

El responsable del archivo establecerá mecanismos para evitar que un usuario pueda acceder a información o recursos con derechos distintos de los autorizados.

La relación de usuarios contendrá el acceso autorizado para cada uno de ellos.

Exclusivamente el personal autorizado podrá conceder, alterar o anular el acceso autorizado, conforme a los criterios establecidos por el responsable del archivo.

f).-Control de acceso físico

Únicamente el personal autorizado podrá tener acceso a los locales donde se encuentran ubicados los sistemas de información.

g).-Gestión de Soportes.

Los soportes informáticos permitirán identificar el tipo de información que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado.

La salida de soportes informáticos que contengan datos de carácter personal, únicamente podrá ser autorizada por el responsable del archivo.

El registro de entrada de soportes informáticos permitirá conocer el tipo de soportes, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y el responsable de la entrega que deberá estar debidamente autorizado.

El registro de salida de soportes informáticos permitirá conocer el tipo de soporte, la fecha y la hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y el responsable de la entrega que deberá estar debidamente autorizado.[93]

Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán medidas necesarias para impedir cualquier recuperación posterior de la información con anterioridad a si baja el inventario.

Cuando los soportes vayan a salir fuera de los locales en que encuentren ubicados los archivos como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada.

h).-Copias de respaldo y recuperación

El responsable del archivo se encargará de verificar la definición y aplicación de los procedimientos de realización de copias de respaldo y recuperación de datos.

[93] Cabe destacar que se pueden presentar verificaciones on line (como por ejemplo en las actuaciones de control sobre páginas web, spam o correos electrónicos etc.

Los procedimientos de copias de respaldo y de recuperación de datos deberán de garantizar su reconstrucción en el estado en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Se realizará una verificación semestral de los procedimientos de copia y recuperación de las copias de respaldo.

Copias de respaldo, al menos semanalmente, salvo que en dicho periodo no se hubieran producido ninguna actualización de datos.

Se conservarán una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan.

i).-Auditoría

Los sistemas de información e instalaciones se someterán a una auditoría interna o externa, que verifique el cumplimiento de las disposiciones aplicables, los procedimientos e instrucciones, al menos cada dos años.

El informe de auditoría dictaminará sobre la adecuación de las medidas y controles, identificará deficiencias y propondrá medidas correctoras o complementarías, se deberá de incluir los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.[94]

Los informes serán analizados por el responsable de la seguridad, que elevará las conclusiones al responsable del archivo para que adopte las medidas correctoras adecuadas quedando a disposición de la agencia de datos.

[94] Dentro de un procedimiento de auditoría se debe establecer como el principal elemento de valoración en cualquiera de sus etapas el grado de incumplimiento de la normatividad sobre protección de datos de carácter personal para así poder tomar las acciones correctivas y preventivas de forma inmediata.

j).-Encargado del tratamiento.

Los servicios prestados por el encargado de tratamiento de datos en su establecimiento deberá de:

I.- Elaborar documentos de seguridad.
II.- Identificación de los archivos tratados.
III.- Identificación del responsable del archivo.
IV.- Identificación de las medidas de seguridad a implementar.

Los servicios prestados por el encargado del tratamiento en los locales del responsable del archivo serán:

1.- Constancia de documento de seguridad.
2.- Compromiso de confidencialidad y cumplimiento de medidas del personal del encargado del tratamiento de los datos.

k).-Prestación de servicios sin acceso:

Adopción de las medidas de seguridad adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de los trabajos que no impliquen el tratamiento de datos personales.

Deberá de recoger de forma expresa en el contrato de prestación de servicios lo siguiente:

La prohibición de acceso a datos de carácter personal o la obligación de guardar secreto.

l).- Prueba con datos reales.

La implantación o modificación de los sistemas de información, las pruebas no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de archivo tratado.

m).-Distribución de soportes

La distribución de los soportes se realizará cifrando los datos, o utilizando cualquier otro mecanismo que garantice la información no sea inteligible ni manipuladora durante su transporte.

n).-Registros de acceso:

De cada acceso se guardaran como mínimo, la identificación del usuario, la fecha y hora en que se realizo, el archivo accedido, el tipo de acceso y si ha sido autorizado o denegado.

En el caso del acceso autorizado, será preciso guardar la información que permita identificar el registro accedido.

Los mecanismos que permiten el registro de los datos detallados en las párrafos anteriores están bajo el control directo del responsable de seguridad, sin que deba permitir, en ningún caso, la desactivación de los mismos.

El periodo mínimo de conservación de los datos registrados el cual se sugiere que sea de dos años

El responsable de la seguridad competente se encargará de revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.

o).-Telecomunicaciones

La transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipuladora.

Se incluyen los archivos adjuntos a los correos electrónicos.

p).- Criterios de archivos de soportes físicos

I.-Relación del archivo físico según la legislación aplicable en cada caso.

II.- Posibilidad de ejercer derechos de acceso, rectificación, cancelación y oposición.

III.- Garantía de correcta conservación.

q).- Traslado de la documentación

Adopción de medidas de seguridad en los traslados físicos de documentos.

r).- Dispositivos de almacenamiento:

Existencia de dispositivos anti manipulación de documentación así como de otras medidas alternativas.

s).-Custodia de los soportes.

Existencia de medidas de seguridad que controle el tráfico transitorio de información.

t).-Almacenamiento de información:

I.-Existencia de áreas protegidas y cerradas con los soportes y archivadores.

II.- Protección de puertas de acceso con sistema de apertura controlado.

III.- Otras medidas de seguridad paliativas.

IV.- Descripción de las mismas en el documento de seguridad, ya sea por:

1.- Copia o reproducción

2.- Control de elementos de reprografía por el personal autorizado.

3.- Control de destrucción de copias y reproducciones incorrectas.

V.-Acceso a la documentación:

Existencia de mecanismos que permiten identificar los accesos realizados en el caso de documentos de uso por una pluralidad de usuarios y el registro de accesos y procedimientos de control de acceso por persona no habitual.

u).- Medidas de seguridad en soporte físico

Considerando que se deberá de aplicar a los archivos lo siguiente:

1.-Los niveles de seguridad

2.-El alcance

3.-Encargados de tratamiento

4.-Prestaciones de servicio sin acceso a datos de carácter personal

5.-Delegación de autorizaciones.

6.-Regimen del trabajo fuera de los locales.

7.- Documentos de seguridad

2.5. Medios de impugnación

De acuerdo a lo dispuesto en el artículo 138 del Reglamento cabe la interposición del juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa en contra de la resolución al procedimiento de verificación.

2.6. Reconducción del procedimiento

En términos del artículo 139 del Reglamento cuando se presente una denuncia y de la misma se desprende que es improcedente el procedimiento de verificación, si no que se actualiza una de las causales de inicio de procedimiento de protección de derechos derivado de una inconformidad por parte del titular por alguna acción u omisión del responsable del tratamiento de los datos con motivo del ejercicio de su derecho de acceso, rectificación, cancelación y oposición se turnará a la Dirección General de Sustanciación y Sanción del Instituto en un plazo no mayor a diez días hábiles contados a partir del día en que se recibió la solicitud.

Conclusión Capitular

En el presente capitulo se desarrollaron los elementos formales, jurídicos y administrativos que el IFAI verifica a los sujetos que tratan y conservan datos personales. Se abordaron los sujetos que intervienen en dicho proceso que en este caso es el IFAI, el titular de los datos personales y el responsable del tratamiento de los datos. Se analizaron las cinco fases del procedimiento las cuales están integradas por la admisión, análisis de oportunidad para realizar la verificación, el desarrollo de la verificación y cierre del acta. Así también se realizo un análisis de los elementos sustantivos que son objeto del procedimiento de verificación de datos como las medidas de seguridad, las obligaciones del personal y la incidencias que se puedan presentar. Por otra parte se señalan otros elementos que son susceptibles de verificar como el control de acceso físico, copias de respaldo, auditorias, controles de acceso a la documentación y medidas de seguridad en un soporte físico. Por último se menciono los medios de impugnación y la explicación de lo que es la reconducción del procedimiento.

CAPÍTULO TERCERO

En el presente capítulo se explicará de manera detallada todo lo concerniente al procedimiento administrativo sancionador por parte del IFAI en contra de los sujetos regulados derivados del procedimiento de verificación, por una denuncia o por el comunicado de otra autoridad. Se plasman definiciones, principios procesales, etapas del procedimiento sancionador, notificaciones, pruebas y su desahogo, alegatos, cierre de la instrucción, resolutivo, criterios para la imposición de las sanciones, medios de impugnación, caducidad, prescripción, fundamentos legales, facultades de la autoridad sancionadora.

Procedimiento administrativo sancionador en materia de protección de datos personales

3.1. Principios

Los principios que constituyen el procedimiento sancionador en materia de protección de datos son los siguientes:[95]

1.- Principio de Legalidad: Es definido como la existencia de preceptos jurídicos que permiten predecir con suficiente grado de certeza aquellas conductas y se sepa que atenerse en cuanto a la conexidad con la responsabilidad y la eventual sanción.

2.- Principio de Tipicidad: Se tiene que tener prevista en una ley la infracción y la sanción.

3.- Principio de Non Bis in Ídem: Consistente en que una persona no puede ser sancionada dos veces por el mismo hecho con sanciones el mismo orden.

[95] TELLEZ Abel. Ref. 09. 224-234 p.

4.-Principio de Irretroactividad: Solo se aplicaran normas sancionadoras de carácter retroactivo cuando favorecen al sancionado.

5.- Principio de Culpabilidad: Se debe acreditar la culpabilidad del sujeto infractor para poder determinar la existencia de una infracción administrativa.

6.-Principio de Proporcionalidad: El cual consiste en limitar la discrecionalidad en el ejercicio de la actividad represiva del Estado.

3.2. Sujetos que intervienen en un procedimiento administrativo sancionador en materia de protección de datos

Generalmente dentro de un procedimiento administrativo sancionador se identifican los siguientes sujetos:

1.- Instituto Federal de Acceso a la Información y Protección de Datos.

2.- Titular de los datos o su representante legal.

3.-Como presuntos infractores se encuentran: El responsable y en el encargado del tratamiento de los datos.

4.- Tercero Interesado: En caso que corresponda sería la persona que acredite el interés jurídico para intervenir en el asunto antes del cierre de la instrucción.

3.3. Procedimiento de imposición de sanciones.

Después de que el IFAI realice las visitas de verificación respectivas y se determinase un incumplimiento a los principios o disposiciones a la LFPDPPP se iniciará el procedimiento de imposición de sanciones.

3.3.1. Etapas del procedimiento

1.- Derivado del procedimiento de protección de derechos o de verificación se notificará al presunto infractor en el domicilio que el IFAI tenga registrado.

El inicio del procedimiento sancionador deberá de contener:[96]

A).- Identificación de la persona presuntamente responsable.

B).- Descripción sucinta de los hechos imputados y la posible conducta a sancionar que pudiera corresponder.

C).- Indicación del órgano competente para resolver el procedimiento.

D)-Indicación del presunto responsable de que puede reconocer voluntariamente su responsabilidad.

E).-Designación del instructor y en su caso el secretario.

F).-Indicación expresa del derecho responsable a formular alegaciones, a la audiencia del procedimiento y a proponer las pruebas que estime pertinentes.

G).- Medidas de carácter provisional que pudieran generarse.

2.- En la notificación se adjuntará el informe en donde se describa los hechos constitutivos de la presunta infracción.

[96] VELEIRO Belén. Ref. 15. 205 p.

3.- Emplazado el presunto infractor contará con un término de 15 días hábiles después de que surta efectos la notificación para hacer las manifestaciones conducentes y aportar las pruebas que estime convenientes.

4.- El presunto infractor en su contestación deberá responder cada uno de los hechos que se le imputan de manera expresa, ya sea que los niegue o los afirme o en su caso que los ignore por no ser propios o rectificando como ocurrieron, presentando los argumentos que traten de desvirtuar la infracción, así como las pruebas que estime pertinentes.

5.- Las pruebas que se pueden ofrecer en materia de protección de datos son las siguientes:

5.1 Documental Pública
5.2 Documental Privada
5.3 Pericial
5.4 Testimonial
5.5 Inspección

5.6.- Para el caso en que se ofrezca la prueba pericial o testimonial deberán determinarse los hechos en que versen señalando el nombre y domicilio del perito o de los testigos y se deberá exhibir el cuestionario respecto, en el caso que se deje de observar lo antes expuesto se tendrán por no ofrecidas dichas pruebas.

5.7.- Al escrito del ofrecimiento de pruebas del presunto infractor deberá recaer un acuerdo de admisión o desechamiento de las mismas. Ahora bien para el caso que aplique se determinará lugar, fecha y hora para el desahogo de las pruebas, que por su especial naturaleza así lo requieran levantando el acta respectiva para dejar constancia de ello.

6.- Cierre de la instrucción. Después de desahogarse todas las pruebas se notificarán al presunto infractor para que en un término de 5 días hábiles presente sus alegatos, dicho plazo será computado al día siguiente en que surta efectos la notificación.

7.- Al concluir el plazo citado en el párrafo anterior será cerrada la instrucción, por lo que el instituto deberá emitir su resolutivo en un término no mayor de cincuenta días hábiles siguientes a los que inicio el procedimiento con la salvedad que bajo una causa justificada, el pleno podrá ampliar por una sola ocasión y hasta por un periodo igual al plazo de cincuenta días hábiles, siempre y cuando lo justifique.

No olvidemos que en el procedimiento sancionador en materia de protección de datos se aplicarán las normas generales del Derecho Administrativo.

3.3.2. Presunción de inocencia

Es relativamente común que en las resoluciones emanadas por las autoridades administrativas o judiciales en materia de protección de datos operen bajo la premisa de que si el imputado ofrece una justificación hipotética de su actuación y está no se puede verificar debe prevalecer el principio de presunción de inocencia sin que el presunto infractor sea sancionado. En aras de garantizar el principio de presunción de inocencia. Por lo antes expuesto es de considerar que no debe imponerse sanción alguna en razón de la culpabilidad del imputado si no existe actividad probatoria de cargo que bajo la apreciación de los órganos o autoridades llamadas a resolver no destruya dicha presunción. Sin embargo, no significa que existiendo una prueba de cargo suficiente obtenida con base en medios probatorios lícitos el sancionado este exento de toda actividad probatoria tendiente a justificar su conducta.[97]

3.3.3. Ponderación del beneficio obtenido por el infractor

El establecimiento de sanciones pecuniarias deberá prever que la comisión de las infracciones tipificadas no resulte más beneficiosa para el infractor que el cumplimiento de las normas infringidas.

[97] ALVAREZ HERNANDO Javier. Guía práctica sobre protección de datos. España. Lex Nova.2011. 543 p.

Se apreciara una cualificada intencionalidad en la culpabilidad o en la reincidencia o se evaluara una agravación de la antijuridicidad del hecho o si el beneficio obtenido superase económicamente el máximo de la sanción prevista para la clase de infracción de que se trate, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que siga inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate.[98]

3.3.4. Apercibimiento

En algunos casos relativos al procedimiento administrativo sancionador en protección de datos personales de manera excepcional y previa audiencia de los interesados, considerando que está atendida la naturaleza de los hechos y la concurrencia significativa de los criterio relativos a la graduación de sanciones, la autoridad podrá no acordar la no apertura del procedimiento sancionador y, en su lugar, apercibir al sujeto responsable a fin de que, en el plazo que el órgano sancionador determine, acredite la adopción de medidas correctoras que en cada caso resulten pertinentes, considerando que concurran los siguiente supuestos:

1.- Que los hechos se encuentren dentro de los supuestos previstos en el artículo 64 Fracción I de la LFPDPPP, es decir que no cumpla debidamente con la solicitud de acceso, rectificación, cancelación y oposición al tratamiento de sus datos personales sin alguna razón debidamente fundada.

2.- Que el infractor no hubiese sido sancionado o apercibido con anterioridad.

Para el caso de que el apercibimiento no fuera atendido en los plazos señalados por la autoridad administrativa, está procederá al inicio del procedimiento administrativo sancionador por su incumplimiento.[99]

[98] SALLA Xavi y ORTEGA Jorge. Ref. 64. 192 p.
[99] ALVAREZ HERNANDO Javier. Ref. 97. 542 p.

3.3.5. Sujetos sancionados

Dentro de la delimitación subjetiva de la responsabilidad de los sujetos del régimen sancionador debemos considerar a los siguientes sujetos en los cuales comenten la descripción de la conducta administrativa sancionada:[100]

1.- El responsable de los archivos: Es la persona física o moral de naturaleza privada, que decide sobre la finalidad, contenido y uso del tratamiento.[101]

2.-El responsable del tratamiento: Es la persona física o moral de naturaleza privada que decide sobre la finalidad, contenido y uso del tratamiento. La diferencia entre este y el anterior estriba en el hecho de que, en este caso no ha de ser necesariamente responsables de un archivo de datos de carácter personal.[102]

3.- El encargado del tratamiento: Es la persona física o moral que solo o conjuntamente con otro trate datos personales por cuenta del responsable del tratamiento.[103]

4.- El responsable subsidiario o solidario: Son aquellas personas físicas y morales que incumplen las obligaciones previstas en la LFPDPPP y su reglamento, que de manera conjunta conlleve el deber de prevenir la infracción administrativa cometida por otros.[104]

3.3.6. Consideraciones de la imposición de la sanciones

La autoridad sancionadora puede realizar una valoración de las circunstancias fácticas cuando se trate de acreditar de manera indubitable la disminución de la culpabilidad o de

---

100 SALLA Xavi y ORTEGA Jorge. Ref. 64. 143 p.

101 El responsable de los archivos es quien decide la creación del archivo, su aplicación, finalidad contenido y uso, es decir quién tiene la capacidad de decisión sobre la totalidad de los datos registrados.

102 Se entiende que este sujeto se le imputan las decisiones sobre las concretas actividades de un determinado tratamiento de datos, esto es, sobre una aplicación específica.

103 Dentro del ámbito de la responsabilidad este sujeto puede destinar los datos a otra finalidad, los comunica o los utilice incumpliendo las estipulaciones previstas en la Ley y su Reglamento, respondiendo a las infracciones que hubiera incurrido personalmente.

104 DÍAZ-ARIAS José Manuel. Guía práctica sobre normativa de protección de datos y publicidad comercial. España. Ediciones Deusto. 2008. 193 p.

la antijuridicidad ello de razón de moderar la cuantía de la sanción. Adicionalmente se debe considerar una adecuada proporcionalidad a la entidad de los hechos sancionados de acuerdo a los siguientes criterios:[105]

1.- Cuando se aprecie una cualificada disminución de la culpabilidad del imputado.

2.- Cuando la entidad infractora haya regularizado la situación anómala en forma diligente.

3.- Cuando pueda apreciarse que la conducta del afectado ha podido inducir a la comisión de la infracción.

4.- Cuando el infractor haya reconocido espontáneamente su culpabilidad.

5.- Cuando se haya producido un proceso de fusión por absorción y la infracción fuese anterior a dicho proceso no siendo imputable a la entidad absorbente.

Los criterios para graduar la cuantía de las sanciones son:[106]

1.- La naturaleza de los derechos personales afectados.

2.-El volumen de los tratamiento efectuados.

3.-Los beneficios obtenidos.

4.-El grado de intencionalidad.

5.- La reincidencia por comisión de infracciones de la misma naturaleza.

[105] ENÉRIZ Francisco Javier y BELTRÁN Juan Luis. Ref. 77. 123 y 124 p.
[106] SALLA Xavi y ORTEGA Jorge. Ref. 64. 603 p

6.- Los daños y perjuicios causados a las personas interesadas y a terceras personas.

7.- El carácter continuado de la infracción.

8.- La acreditación de que con anterioridad a los hechos constitutivos de la infracción, la entidad imputada tenía implantados procedimientos adecuados de actuación en la obtención y tratamiento de los datos de carácter personal, siendo la infracción consecuencia de una anomalía en el funcionamiento de dichos procedimientos no debida a una falta de diligencia exigible al infractor.

9.- Cualquier circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad en la actuación del infractor.

En palabras de Patón Pérez un sistema que conjugara la gravedad de la infracción con la capacidad financiera de la empresa en la determinación de la cuantía de la multa sería más equitativo.[107]

La existencia de sanciones efectivas y disuasorias son importantes a la hora de garantizar la observancia de las normas, al igual que lo son los sistemas de verificación directa por las autoridades, los auditores o los servicios de la administración encargados específicamente de la protección de datos.

3.3.7. Infracciones y sanciones

Las infracciones y sanciones previstas en la LFPDPPP en las cuales pueden incurrir los responsables del tratamiento de los datos son las siguientes:

> *Artículo 63.- Constituyen infracciones a esta Ley, las siguientes conductas llevadas a cabo por el responsable:*

[107] Ibídem 193 p.

I. No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada, en los términos previstos en esta Ley;

II. Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales;

III. Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable;

IV. Dar tratamiento a los datos personales en contravención a los principios establecidos en la presente Ley;

V. Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16 de esta Ley;

VI. Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares;

VII. No cumplir con el apercibimiento a que se refiere la fracción I del artículo 64;

VIII. Incumplir el deber de confidencialidad establecido en el artículo 21 de esta Ley;

IX. Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin observar lo dispuesto por el artículo 12;

X. Transferir datos a terceros sin comunicar a éstos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos;

XI. Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable;

XII. Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley;

XIII. Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible[108]*;*

XIV. Obstruir los actos de verificación de la autoridad;

XV. Recabar datos en forma engañosa y fraudulenta;

XVI. Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el Instituto o los titulares;

[108] Cabe mencionar que al respecto al empresa Google ha recabado datos de carácter personal sin permiso de los usuarios desde 2007 durante la elaboración del archivo fotográfico de Google Street View, ello en razón del reconocimiento de que los automóviles que utilizo en la toma de imágenes también capturaban correos electrónicos y otras informaciones personales enviadas a través de redes wifi sin contraseña.

XVII. Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos de acceso, rectificación, cancelación y oposición establecidos en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos;

XVIII. Crear bases de datos en contravención a lo dispuesto por el artículo 9, segundo párrafo de esta Ley, y

XIX. Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto en la presente Ley.

Artículo 64.- Las infracciones a la presente Ley serán sancionadas por el Instituto con:

I. El apercibimiento para que el responsable lleve a cabo los actos solicitados por el titular, en los términos previstos por esta Ley, tratándose de los supuestos previstos en la fracción I del artículo anterior;

II. Multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones II a VII del artículo anterior;

III. Multa de 200 a 320,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones VIII a XVIII del artículo anterior, y

IV. En caso de que de manera reiterada persistan las infracciones citadas en los incisos anteriores, se impondrá una multa adicional que irá de 100 a 320,000 días de salario mínimo vigente en el Distrito Federal. En tratándose de infracciones cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces, los montos establecidos.

Es importante mencionar que en legislaciones como la Española en determinados supuestos de infracciones muy graves[109] derivados de la utilización o cesión ilícita de datos de carácter personal en los que se atente contra el libre ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad, la autoridad administrativa además de ejercer la potestad sancionadora, requerirá a los responsables de los archivos para que cese inmediatamente la utilización o tratamiento de los datos, por lo que en caso de no cumplir con ello la autoridad tiene la facultad de inmovilizar los archivos o cancelación de las bases de datos con la finalidad de restaurar los derechos de las personas afectadas.[110]

[109] Las sanciones muy graves de acuerdo a la Ley de Protección de datos en España 15/99 corresponden a la recolección de datos de forma engañosa y fraudulenta. Realización de comunicación o cesión de datos fuera de las cosas en que estén permitidas. No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido por el Director de la Agencia de Protección de Datos. Tratar datos de carácter personal de forma ilegítima o menospreciando los principios o garantías aplicables, impidiendo o atentando contra el ejercicio de sus derechos fundamentales. Vulnerar el deber de guardar secreto sobre los datos de carácter personal, así como los que hayan sido recabados para fines policiales son consentimiento de las personas afectadas. No atender u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición. No atender el deber legal de notificación de la inclusión de datos de carácter personal en un fichero. Las sanciones aplicables serán de 300,506. 05 € a 601,012.10 €.

[110] BUREAU VERITAS Formación. Ley de Protección de datos personales. Manual práctico para la protección de los datos personales de las personas físicas. España. Fundación CONFEMETAL. 2009. 212 p.

3.3.8. Caducidad

De acuerdo a lo establecido en el articulo 5 párrafo segundo de la LFPDPPP en los procedimientos de protección de derechos, de verificación e imposición de sanciones se observarán las disposiciones previstas en la Ley Federal del Procedimiento Administrativo. Es por ello que conforme a los dispuesto en el artículo 60 del citado ordenamiento se genere en los procedimientos iniciados a instancia del interesado, y se produzca la paralización por causas imputables al mismo después de transcurridos tres meses se producirá la caducidad del mismo. En consecuencia al expirar dicho plazo sin que el interesado requerido realice las actividades necesarias para reanudar la tramitación la autoridad acordará el archivo de actuaciones con la debida notificación al interesado.

Cabe hacer mención que la caducidad no produce por sí misma la prescripción de las acciones del particular.

Por otra parte cuando se trate de procedimientos iniciados de oficio se entenderán caducados y se procederá al archivo de actuaciones a solicitud de parte interesada o de oficio, en el plazo de 30 días contados a partir de la expiración del plazo para dictar resolución.

3.3.9. Prescripción

De acuerdo a lo establecido en el articulo 5 párrafo segundo de la LFPDPPP en los procedimientos de protección de derechos, de verificación e imposición de sanciones se observarán las disposiciones previstas en la Ley Federal del Procedimiento Administrativo. Es por ello que conforme a los dispuesto en el artículo 79 del citado ordenamiento la facultad de la autoridad para imponer sanciones administrativas prescribe en cinco años. Adicionalmente se debe considerar que los términos de la prescripción serán continuos y se contarán desde el día en que se cometió la infracción

administrativa si fuere consumada o, desde que ceso si fuere continúa. Cabe hacer mención que si el presunto infractor impugna los actos de autoridad administrativa interrumpirá la prescripción hasta en tanto la resolución definitiva se dicte o no admita ulterior recursos.

3.3.10. Recursos administrativos

En contra de la resolución que generé el Pleno del Instituto derivado del procedimiento de imposición de sanciones cabe la interposición del juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa, ello conforme a lo dispuesto en el artículo 144 del Reglamento de la LFPDPPP.

Conclusión Capitular

En razón de la temática desarrollada en el presente capítulo se determinaron los principios que rigen el procedimiento administrativo sancionador en materia de protección de datos personales. Así también se determino los sujetos que intervienen en dicho procedimiento. Un aspecto toral es la descripción detallada de las etapas del procedimiento comenzando por los elementos formales con que se inicia el procedimiento, notificaciones, pruebas, apercibimientos, sujetos sancionados. Adicionalmente se realizo un análisis de ciertas consideraciones que deben aplicarse al momento de imponer las sanciones. Por último se describieron las infracciones y los recursos administrativos que en su momento procedan.

CAPÍTULO CUARTO

Todos aquellos particulares que manejan datos personales necesitan de un referente sistematizado o un punto de referencia del cual puedan partir para implementar una estructura que garantice la seguridad de los datos personales. Es por ello que en este capítulo se explicará aspectos específicos aspectos metodológicos convenientes y eficaces que coadyuvan a reducir cualquier vulneración o algún tipo de incidente que tenga consecuencias desfavorables en el tratamiento y custodia de las base de datos personales. Por lo tanto se expondrán aquellas actividades coordinadas que dirigen y controlan ciertos procesos en una organización que permitan mantener vigente e incluso mejorar la protección de datos personales.

4.1. Sistema de gestión de seguridad de datos personales

El artículo 19 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares establece la obligación para todo responsable que lleve a cabo el tratamiento de datos personales, de implementar y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra cualquier tipo de daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado de los mismos.

Por lo antes expuesto el IFAI de acuerdo con las atribuciones con las que cuenta se ha dado a la tarea de divulgar estándares y mejores prácticas internacionales en materia de protección de datos personales, razón por la cual ha establecido recomendaciones en materia de seguridad de la información para los sujetos regulados. Es por ello que específicamente en lo concerniente a la implementación de procedimientos y mecanismos que coadyuven con las mejores de seguridad de datos personales[111] y se valoren ciertas

[111] El Pleno del Instituto Federal de Acceso a la Información y Protección de Datos, con fundamento en lo dispuesto por los artículos 19, 39, fracción IV de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; 58 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; 15, fracciones I y XXI, 24, fracción III, y 30, fracción II del Reglamento Interior del Instituto Federal de Acceso a la Información y Protección de Datos publicado en el Diario Oficial de la

amenaza pueda explotar las vulnerabilidades de un activo o grupo de activos en perjuicio de la organización para efectos de disminuir dichas potencialidades que son consideradas como riesgos de seguridad.

Ahora bien el IFAI recomiendo la implementación de un sistema de gestión en materia de seguridad de datos personales en lo sucesivo se le denominar como "SGSDP" el cual se define como un sistema general creado por una organización la cual puede ser una persona física o una persona de carácter moral para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales en función del riesgo de los activos y de los principios básicos de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad previstos en la Ley, su Reglamento, normatividad secundaria y cualquier otro principio en cuanto a la implementación de buenas prácticas respecto a las disposiciones regulatorias que a nivel internacional estipule en la materia.[112]

Debemos de considerar que un sistema de gestión[113] apoya a las organizaciones en la dirección, operación y control de forma sistemática y transparente de sus procesos, a fin de lograr el cumplimiento de las disposiciones establecidas en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento.

El sistema de gestión propuesto se basa en el modelo denominado "Planificar-Hacer-Verificar-Actuar" en lo sucesivo (PHVA) a través del cual se dirigen y controlan los procesos o tareas en materia de protección de datos personales y fomentar las buenas prácticas de acuerdo al siguiente proceso y actividades:

PROCESO	Elemento del SG	Fase del PHVA	ACTIVIDADES

Federación el 30 de Octubre de 2013 bajo el rubro de recomendaciones en materia de seguridad de datos personales, mismo que fue consultado en http://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013.

112 Ídem.

113 Un Sistema de Gestión define como un conjunto de elementos y actividades interrelacionadas para establecer metas y los medios de acción para alcanzarlas.

	Metas	Planificar	Se identifican políticas, objetivos, riesgos, planes, procesos y procedimientos necesarios para obtener el resultado esperado por las personas físicas o morales (meta).
	Medios de acción	Hacer	Se implementan y operan las políticas, objetivos, planes, procesos y procedimientos establecidos en la fase anterior.
		Verificar	Se evalúan y miden los resultados de las políticas, objetivos, planes, procesos y procedimientos implementados, a fin de verificar que se haya logrado la mejora esperada.
		Actuar	Se adoptan medidas correctivas y preventivas, en función de los resultados y de la revisión, o de otras fuentes de información relevantes, para lograr la mejora continua.

Dentro de las acciones mínimas que se tienen que desarrollar en un SGSDP, en materia de protección de datos personales se deberán de considerar las siguientes acciones:

4.1.1. Fase 1 planeación

Alcance y objetivos

Es este rubro deben fijarse en función de la fuente de los datos personales, es decir determinar si se recaban directamente del titular o provienen de una transferencia de datos o de fuentes de carácter público. Aunado a lo anterior se debe considerar los departamentos involucrados y los empleados que están autorizados para tratar datos personales, así como la finalidad en el tratamiento de los mismos, y en su caso determinar con quien se comparten los datos. Es de especial consideración la determinación del donde y como se almacenan los datos personales, así como delimitar los procedimientos tecnológicos utilizados en el tratamiento. En consecuencia se deben considerar un periodo de conservación de los mismos, y por ende tener establecido un procedimiento para destrucción de los mismos.

En cuanto a los objetivos se debe de tomar en consideración varios factores que a continuación se describen:[114]

A) Factores contractuales los cuales se determinan a partir del flujo de información de los datos personales derivados de relaciones de tipo contractual y legal.[115]

B) Factores legales y regulatorios se encuentran previstos en la LFPDPPP y su Reglamento, leyes de protección al consumidor, leyes de notificación de vulneraciones, leyes laborales.

C) Factores en función del modelo de negocios: Estos pueden entenderse como un código de conducta o mejores prácticas de un sector específico que utilice la organización.

D) Factores de carácter tecnológico: Los cuales son concebidos como el conjunto de recursos, procedimientos y técnicas usadas en el procesamiento, almacenamiento y transmisión de datos personales.

4.1.1.1. Política de gestión de datos personales

Los citados numerales coadyuvan con el cumplimiento de lo dispuesto en el artículo 57 del Reglamento de la LFPDPPP el cual refiere que los sujetos regulados deberán establecer y mantener las medidas de seguridad administrativas, físicas y, en su caso, técnicas para la protección de los datos personales.

La política de gestión de datos personales debe considerar el estricto cumplimiento de las disposiciones normativas aplicables en materia de protección de datos personales, debiendo considerar a todos los sujetos involucrados en el tratamiento de los mismos,

114 Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales Septiembre 2013 emitido por el IFAI, págs. 9 y 10

115 Cabe destacar que el tratamiento de datos personales que tiene como objeto cumplir con una obligación derivada de una relación jurídica no será considerada para uso exclusivamente personal; ello de acuerdo a lo dispuesto en el artículo 6 del Reglamento de la LFPDPPP.

debiendo considerar que se deben de integrar para su elaboración los siguientes aspectos:[116]

A).- Se deben considerar los principios de licitud, calidad, información, lealtad, consentimiento, proporcionalidad, responsabilidad y finalidad.[117]

B).- Establecer y mantener medidas de seguridad.

C).- Guardar la confidencialidad de los datos personales.

D).- Se debe establecer un diagrama de flujo y ciclo de vida de los datos personales.

E).- Elaborar un inventario pormenorizado y actualizado de datos personales, elaborando un esquema de categorías que utiliza la organización.

F).- Establecer un mecanismo de protección de derechos de los titulares respecto de sus datos personales.

G).- Considerar las excepciones contempladas en la legislación de datos personales.

H).- Implementar y desarrollar un SGSDP que sean coincidente con la política de protección de datos.

I).- Asignar responsabilidades perfectamente delimitadas a los miembros de la organización en la que se debe establecer un mecanismo de rendición de cuentas al SGSDP.

4.1.1.2. Funciones y obligaciones del responsable o de aquellos sujetos que tratan los datos personales

En este rubro el responsable debe considerar que dentro de los valores de la organización se deben establecer como mínimo las siguientes acciones:

A).- Comunicar a los involucrados en el tratamiento de datos personales la importancia de cumplir con la política de gestión de datos personales, así como el conocimiento pleno de los objetivos del SGSDP y establecer mecanismos de mejora continúa.

---

116 Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales Septiembre 2013 emitido por el IFAI, pág. 11.

117 Los principios aquí expuestos se encuentran plasmados en los artículos 6 de la LFPDPPP y 9 de su Reglamento.

B).- Asignar roles y responsabilidades dentro de la estructura organizacional, implementando una cadena de rendición de cuentas en el SGSDP.

C).- Cerciorarse que los miembros de la organización conozcan perfectamente sus roles y funciones; así como la contribución que pueda generar cada uno de ellos para lograr los objetivos del SGSDP.[118]

Adicionalmente de lo antes expuesto podemos advertir que el numeral 1.3. coadyuva con el cumplimiento de lo dispuesto en los artículos 59 y 61 Fracción II del Reglamento de la LFPDPPP. Es por ello que el responsable del tratamiento de los datos podrá desarrollar las funciones de seguridad por sí mismo, o bien contratar a una persona física o moral para tal fin y así estar en posibilidades de determinar con ello sus respectivas las funciones y obligaciones.

4.1.2. Inventario de datos personales

El inventario de datos personales debe identificar plenamente la información básica que permite conocer a profundidad el tratamiento el tratamiento a que son sometidos los datos personales, ello de acuerdo a las siguientes acciones:[119]

A).- Adquisición de datos personales.

B).-Uso de datos personales en los que se tiene que considerar el acceso, manejo, aprovechamiento, monitoreo y procesamiento.

C).- Divulgación debiendo considerar los actos de transferencia y remisión de los datos personales.

---

[118] Por lo general todas las áreas de involucradas dentro de un SGSDP en una organización son la Dirección, Área de Finanzas y Contabilidad, Recursos Humanos, Tecnologías de la Información y Comunicación, Área legal, Auditoría Interna, Terceros que tienen alguna injerencia directa con las actividades de la organización y todo el Personal de Infraestructura.

[119] Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales Septiembre 2013 emitido por el IFAI, págs. 12 y 13.

D).- Almacenamiento de los datos personales.

E).- Bloqueo de los datos personales.

F).- Cancelación, supresión y en su caso destrucción de los datos personales.

No se debe restar importancia a la categoría que la organización debe hacer de los datos personales debiendo considerar el daño que se podría causar a su titular o a la organización en caso de una vulneración a su seguridad.[120] En lo que respecta a este rubro establece el cumplimiento de lo dispuesto en el artículo 61 Fracción II del Reglamento de la LFPDPPP, en razón de que establece la obligatoriedad de elaborar un inventario de datos personales, así como la implementación de un sistema de tratamiento de datos personales.

4.1.2.1. Análisis de riesgo de los datos personales

A.- Factores para Determinar las Medidas de Seguridad.
B.- Valoración Respecto al Riesgo.

Los datos personales siempre están expuestos a ciertos riesgos de seguridad los cuales no se pueden erradicar en su totalidad. Sin embargo, se puede minimizar a través de ciertos mecanismos establecidos en procesos de mejora continua. Por lo antes expuesto se han establecido criterios de evaluación del riesgo de acuerdo a las medidas de seguridad que se deben de implementar para el resguardo de datos personales de los cuales podemos mencionar los siguientes:[121]

120 Se puede establecer una categorización de los datos personales según su riesgo, siendo esta los datos con riesgo inherente bajo como nombre, teléfono, edad, sexo, RFC, CURP. Datos con riesgo inherente medio como la dirección física y datos de carácter patrimonial de una persona, información biométrica y antecedentes penales. Datos con riesgo inherente alto son aquellos datos personales sensibles, que de acuerdo a la ley incluyen datos de salud, los cuales se refieren a la información médica del titular. Datos con riesgo inherente reforzado siendo estos datos de mayor riesgo, lo que conlleva más beneficio para un posible atacante al obtener un beneficio económico o reputacional como pueden ser los códigos de seguridad, datos de banda magnética o número de identificación personal.

121 Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales Septiembre 2013 emitido por el IFAI, pág. 16.

A).- Los requerimiento regulatorios y contractuales que definen los objetivos del SGSDP.

B).- El valor de los activos en el manejo de datos personales.

C).- Las consecuencias negativas que pueden derivar en la vulneración de los datos personales.

D).- Los posibles daños a la integridad de los titulares de los datos personales.

Existen dos criterios para la evaluación del riesgo, mismos que a continuación se detallan:

A).- Criterios de impacto: Estos se determinan en función del posible nivel del daño, así como el perjuicio causado al titular y el emana de una violación a la seguridad de los datos personales.

B).- Criterios de aceptación del riesgo: En estos se aceptan o no ciertos niveles de riesgos que por su naturaleza son considerados como poco significativos debiendo de considerar para ello las políticas de la organización respecto al tratamiento de los datos personales, los factores tecnológicos, los aspectos legales y regulatorios, así como ciertos factores humanos y sociales.

La identificación de posibles amenazas, algún tipo de vulneración, así como el análisis de los controles existentes son determinados por la valoración del riesgo, el cual ayuda a establecer resultados, consistentes, validos y comparables. La valoración del riesgo se realiza mediante la identificación de los activos que forman parte del ciclo de vida de los datos personales. Los activos antes mencionados se clasifican en primarios y de apoyo, el primero de ellos corresponde en si a los datos personales y su flujo dentro de la organización. El segundo se materializa en el hardware, software, redes, personal y estructura organizacional.[122]

[122] Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales Septiembre 2013 emitido por el IFAI, págs. 17 y 18.

Es importante hacer mención de la diferencia que puede existir de amenazas y riesgos.[123] El primero de ellos se identifica por existir situaciones en las que alguna persona malintencionada pretende acceder fraudulentamente a unos datos personales, para obtenerlos, falsificarlos o manipularlos. Por el contrario, llamamos riesgos a aquellas prácticas incorrectas por parte de los usuarios de los datos personales que pueden poner en peligro su seguridad, sin que hubiese, en principio, alguien que persiguiese activamente ese acceso a los datos.[124]

Uno de los principales objetivos que tiene un SGSDP para establecer el mecanismo de valoración de riesgos es para identificar posibles escenarios de vulneración previstos en el artículo 63 del Reglamento de la LFPDPPP como puede ser la pérdida o destrucción no autorizada, el robo o extravió de información de datos personales; así como el uso, tratamiento o acceso no autorizado o algún daño o alteración.

Con estos numerales se establecen el cumplimiento de lo dispuesto en los artículos 60, 61 Fracciones III y IX, 65 Fracciones I, II, III y IV del Reglamento de la LFPDPPP. Estos atienden a un mecanismo de análisis de riesgos de datos personales en los que se identifique los peligros y se estime los riesgos a los datos personales. Es importante además que se implemente un registro de los medios de almacenamiento de los datos personales. Así también se debe considerar los vulneraciones de seguridad en cualquier fase del tratamiento de los datos, como puede ser la pérdida o destrucción no autorizada, el robo, extravío o copia no autorizada, el uso, acceso o tratamiento no autorizado, así como el daño, la alteración o modificación no autorizada.

4.1.2.2. Identificación de las medidas de seguridad y análisis de brecha

Con la finalidad de disminuir los riesgos contra una vulneración o amenaza a los datos personales se deben de implementar medidas de seguridad las cuales se clasifican de

[123] Hay abundantes ejemplos de amenazas y riesgos. Por no citar más que uno de cada caso, los ataques de piratas informáticos, llamados hackers, en Internet para acceder a bases de datos serían un ejemplo de amenazas, mientras que los escándalos relacionados con listados de datos confidenciales que se han dejado en la basura serían un ejemplo de riesgos por malas prácticas.

[124] Agencia de Protección de Datos de la Comunidad de Madrid, Seguridad de Protección de Datos Personales, Ed. Agencia de Protección de Datos de Madrid, 2009 Madrid España. Pág. 107.

acuerdo a carácter técnico, administrativo o físicas debiendo de considerar los siguientes aspectos para su implementación:

A.- Políticas del SGSDP

B.- Cumplimiento legal

C.- Estructura organizacional de la seguridad

D.- Clasificación y acceso de los activos

Aunado a lo anterior la organización debe establecer dentro del SGSDP ciertas medidas de seguridad que eviten el uso o acceso no autorizado, protejan los datos personales contra daño o pérdida e impidan la divulgación no autorizada de datos personales.

Después de considerar los elementos expuesto en el presente numeral se debe de proceder a determinar el análisis de brecha mediante la identificación de las medidas de seguridad que operan correctamente y las faltantes. Es importante identificar también si se pueden proponer nuevas medidas de seguridad que puedan remplazar a algún tipo de control que se puedan implementar. No obstante lo anterior debemos considerar el nivel de cumplimiento de cada control con el objeto de identificar el nivel de madurez. Con el objeto de evaluarlos de deben establecer ciertos controles ello de acuerdo a la naturaleza de los siguientes niveles:

A).- Documentados

B).- Registros

En el numeral que antecede se deberá de considerar la distinción de archivos o ficheros de tipo físico, lógico y jurídico, para determinar la finalidad o propósito con la que se trata los datos personales que se contienen en los mismos ello con el objeto de determinar las medidas de seguridad más idóneas.[125]

[125] El fichero lógico es aquel que resulta de la organización interna de un sistema de información de acuerdo con las características de almacenamiento en un soporte informático o electrónico, siendo que la ubicación de estos ficheros da lugar a la definición de fichero físico. El fichero jurídico es aquel por la finalidad o propósito con las que se tratan los datos personales.

A.- Seguridad del personal

B.- Seguridad física y ambiental

En este rubro se debe de considerar el establecimiento de medidas de seguridad en sistemas de datos personales de acuerdo a una clasificación de nivel básico, medio y avanzado.[126]

A.- Gestión de comunicaciones y operaciones

B.- Control de acceso

C.- Desarrollo y mantenimiento de sistemas

D.- Vulneraciones de seguridad

De acuerdo a lo establecido en los puntos anteriores se concluye el cumplimiento cabal de acuerdo a lo dispuesto en los artículos 61 Fracción IV y V del Reglamento de la LFPDPPP. Lo anterior se afirma en razón de que se establecen las medidas de seguridad aplicables a los datos personales y se identifican aquéllas implementadas de manera efectiva, considerando también el análisis de brecha mismo que consiste en determinar la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales.

4.2. Fase 2.- Implementar y operar el SGSDP

4.2.1. Implementación de las medidas de seguridad aplicables a los datos personales.

En este rubro se debe establecer una metodología de análisis de riesgo para reforzar o establecer medidas de seguridad o cuales activos se encuentran más expuestos debiendo considerar tres variables que afectan la percepción del valor de los datos personales para

[126] El nivel básico de seguridad se aplica a todos los sistemas que contengan datos de carácter personal, el nivel medio corresponde a aquellos sistemas corresponden a aquellos sistemas que proporcionan un perfil de la persona y permiten evaluar varios aspectos de su personalidad, tales como rendimiento laboral o crediticio, en cuanto al nivel alto son aquellos sistemas que contienen información sobre origen étnico, racial, estado de salud físico, creencias y convicciones religiosas o filosóficas. Cabe mencionar que los niveles de seguridad antes mencionados son acumulativos en el sentido en el que los sistemas de datos personales de nivel alto tienen que cumplir con las de nivel medio y básico.

un sujeto que pretenda vulnerarlos de acuerdo a lo establecido en la fase de planeación, por lo anterior se debe de considerar las siguientes variables:[127]

A) Beneficio para el atacante: Son aquellos datos personales que representan un mayor beneficio para el atacante.

B) Accesibilidad para el atacante: Aquellos datos personales que sean de fácil acceso tienen mayor posibilidad de ser atacados.

C) Anonimidad del atacante: Aquellos datos personales cuyo acceso represente mayor anonimidad tienen más probabilidad de ser atacados.

4.2.2. Cumplimiento cotidiano de medidas de seguridad

Se deben establecer mecanismos por parte de los miembros de la organización para efectos de que manera diaria se esté realizando un monitoreo para validar el cumplimiento de las políticas y gestión de calidad en materia de protección de datos personales, ello se logra con el estableciendo un compromiso total del cumplimiento, desarrollo y revisión y aseguramiento de la implementación de la política, así como las revisiones de gestión de la misma.[128]

Ahora bien otro aspecto importante a considerar en este rubro es la aprobación de procedimientos por parte del SGSDP en los que se debe de observar la correcta administración y comunicación de los avisos de privacidad correspondiente. El manejo optimo respecto de las solicitudes en el ejercicio de los derechos ARCO por parte de los titulares, recolección y manejo de los datos personales. El procedimiento del manejo de posibles quejas, así como el manejo de incidentes de seguridad.

---

127 IFAI, Metodología de Análisis de Riesgo BAA, Septiembre de 2013, documento electrónico consultado el día 27 de Diciembre de 2013 en la siguiente dirección electrónica http://inicio.ifai.org.mx/DocumentosdeInteres/Metodologia_de_Analisis_de_Riesgo_BAA_nuevo_aviso.pdf; pág. 2

128 Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales Septiembre 2013 emitido por el IFAI, pág. 22.

Así también se debe de contemplar que se asigne a un miembro de la organización para los tramites y asesoramiento de los asunto relacionados con el IFAI. Adicionalmente este miembro verificará las relaciones que se establezcan con otras organizaciones para el caso de la transferencia de datos personales ya sea entes nacionales o internacional de carácter privado.

El SGSDP debe considerar ya sea por asesoría externa o mediante la asignación de un abogado de la organización para efectos de que apoye con la asesoría legal y la actualización de la legislación nacional e internacional en materia de datos personales. Lo anterior con el objeto de otorgar la asesoría legal a los integrantes de la organización, así como gestionar los procedimientos jurídicos-administrativos de acuerdo a la tutela efectiva de derechos por parte de los titulares de datos personales, así como aquellos procedimientos de verificación o el procedimiento administrativo sancionar que pueda incoar en contra de la Organización.

4.2.3. Plan de trabajo para la implementación de las medidas de seguridad faltantes

Del numeral antes expuesto se advierte el cumplimiento de lo dispuesto en los artículos 59, 61 Fracción IV y VI del Reglamento de la LFPDPPP, en razón de que se establecen y mantienen de manera efectiva las medidas de seguridad, así como la implementación de medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva; así como la elaboración de un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha.

4.3. FASE 3.- Monitorear y revisar el SGSDP

La fase de monitoreo y revisión se constituyen de las siguientes fases:

4.3.1. Revisión de los Factores de Riesgo.

4.3.2. Auditoría ya sea de carácter interno o externo.

4.3.3. Vulneraciones a la Seguridad de la Información.

Al tenor del numeral que antecede se cumple con lo requerido en los artículos 61 Fracción VII, 62 Fracciones I, II, III y IV del Reglamento de la LFPDPPP. Toda vez que se cuenta un plan de trabajo para la implementación de las medidas de seguridad faltantes derivadas del análisis de brecha. Asimismo se establece la actualización de las medidas de seguridad cuando se modifiquen las medidas o procesos de seguridad para su mejora continua. Ahora bien derivado de las revisiones a la política de seguridad del responsable debe verificar que se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo. Lo anterior evita que se vulneren los sistemas de tratamiento de los datos personales o que exista una afectación a los datos personales distinta a las anteriores. Es de considerar que para el caso de que los datos personales sean sensibles, los responsables procurarán revisar y, en su caso actualizar las relaciones correspondientes una vez al año.

4.4. FASE 4.- Mejorar el SGSDP

4.4.1. Programas de mejora en la capacitación al personal para mantener la vigencia del SGSDP

Por último en cuanto a la fase de mejora del SGSDP se cumple con lo dispuesto en los artículos 61 Fracción VIII, 64, 65 y 66 del Reglamento de la LFPDPPP. Lo anterior se determina de acuerdo a la capacitación del personal que intervenga en el tratamiento. Así también se considera la obligación de informar al titular de los datos sobre las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales. En cuanto confirme que ocurrió la vulneración y haya tomado las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación sin dilación alguna a fin de que los titulares afectados puedan tomar las medidas correspondientes.

En otro orden de ideas se debe considerar la naturaleza del incidente y los datos personales comprometidos. Por lo tanto se deben generar las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses, las acciones correctivas realizadas de forma inmediata. Ahora bien se debe considerar que para el

caso de que ocurra una vulneración a los datos personales, el responsable deberá analizar las causas por las cuales se presentó e implementar las acciones correctivas, preventivas y de mejora para adecuar las medidas de seguridad correspondientes a efecto de evitar que la vulneración se repita.

Conclusión Capitular

En el presente capitulo de identificaron las partes más representativas de los procesos de un Sistema de Gestión sobre protección de datos personales. Comenzando por la planeación y las principales actividades de los responsables que tratan datos personales, inventario de los datos personales. Así también se explico a detalle el análisis de riesgos que pueden sufrir los datos personales y la identificación de las medidas de seguridad que deben implementarse en las áreas en que traten y almacenen datos personales. Por otra parte se hace la propuesta sobre la implementación de medidas de seguridad faltantes así como el monitoreo del sistema de gestión sobre protección de datos personales en que ha implementado. Por último se hace una propuesta para generar programas de capacitación y mejora continua en el sistema de merito.

CAPÍTULO QUINTO

La imagen de un ser humano atiende a la fisonomía que tenemos las personas lo que permite que un individuo sea único e irrepetible siendo un reflejo de caracteres esenciales de una persona; por lo que cada individuo tenemos la facultad de autodeterminación respecto de la captación, reproducción y publicación de su propia imagen, donde, cómo y cuándo desee; siendo esto un aspecto positivo del manejo de la propia imagen; desde un aspecto negativo y traducido en un derecho subjetivo que las personas tenemos respecto de nuestra propia imagen podemos impedir la obtención, adaptación o reproducción de la figura humana por terceros sin el respectivo consentimiento. El derecho a la intimidad personal tiene por objeto garantizar al individuo un ámbito reservado de su vida , el cual es excluido del conocimiento como de las intromisiones de terceros.

Regulación de la videovigilancia

5.1. Videovigilancia y datos personales

Uno de los países que presentan una vasta regulación en materia de videovigilancia es España. Por ello es importante mencionar la protección que la Constitución Española consagra en el artículo 18.1 en la cual indica que la propia imagen es un derecho de la personalidad derivado de la dignidad humana, y el cual está dirigido a proteger la dimensión moral de las personas que atribuye a su titular un derecho a determinar la información gráfica generada por los rasgos físicos personales que pueden tener en la dimensión pública.[129]

Ahora bien en muchos sitios públicos y privados encontramos videocámaras que captan imágenes diversas entre ellas imágenes corporales de las personas perfectamente

[129] Sentencia del 24 de Julio de 2012 emitida por el Tribunal Supremo de Madrid Caso respecto de la demanda interpuesta por Elsa Pataky en contra de varios medios de comunicación por violación a su propia imagen.

identificables, que en algunos casos desconocen que su imagen está siendo captada. En otras ocasiones se obtienen imágenes en tiempo real o son grabadas y resguardadas en un centro de datos como es el caso de la videovigilancia administrada.[130]

El fenómeno antes expuesto es conocido como videovigilancia mismo que es necesario definir para efectos de un mejor entendimiento de lo que aquí se desarrollará. Es por ello importante señalar el criterio de Ernesto Sánchez con respecto a la videovigilancia la cual define como un conjunto de tecnologías y productos de su desarrollo, mismas que permiten realizar la función de vigilancia que en condiciones que antes el hombre, por ciertas limitaciones naturales no podía llevar a cabo. Este sistema permite captar imágenes fijas o en movimiento con un mayor alcance, visión, resolución posibilitando su almacenamiento, consulta y tratamiento, el cual puede desarrollarse dependiendo del estado actual de la tecnología.[131]

Es de considerar que la videovigilancia pretende garantizar la seguridad patrimonial o la integridad de personas físicas o morales ya sea de carácter público o privado; y en algunos de los casos la videovigilancia se utiliza para verificar el cumplimiento de ciertas obligaciones como la observancia a un reglamento de tránsito o en materia de seguridad bancaria así resguardo de algún inmueble ya sea público o privado.

La captación y el tratamiento de imágenes mediante la videovigilancia conlleva una invasión a la intimidad en razón de que repercute sobre las excepciones personales en materia de derecho a la información. Lo anterior atiende a la captación de imágenes de personas identificables o identificadas sin que puede actualizarse un procedimiento de la disociación de los datos personales, y que en su momento se materializa como una violación de los derechos fundamentales como es la invasión a la privacidad de acuerdo a lo establecido en el artículo sexto de la Constitución Política de los Estados Unidos Mexicanos, segunda fracción misma que señala lo siguiente: “La información que se

130 Servicio de video monitoreo basada en una aplicación IP, que ofrece a las empresas la capacidad de visualizar cámaras de video analógicas ó IP, así como, grabar video en tiempo real bajo un esquema centralizado y resguardado en el Data Center como es el caso de la Empresa Teléfonos de México (Telmex).

131 Ibarra Sánchez Ernesto “Videovigilancia” Punto de Colisión entre Derechos Fundamentales, Seguridad y Protección de Datos Personales en México, Acervo de la Biblioteca Jurídica de la UNAM, consultada el día 21 de Enero de 2013 en http://biblio.juridicas.unam.mx/libros/6/2958/17.pdf.

refiere a la vida privada y los datos personales serán protegida en los términos y con las excepciones que fijen las leyes". Otra disposición constitucional es aquella dispuesta en el artículo 16 del citado precepto normativo en el sentido de que: "Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición en los términos que fije la Ley".

Derivado de lo anterior es imprescindible considerar la aplicación de la Ley de Protección de Datos Personales en Posesión de los Particulares para el caso de la captación y transferencia de información de las imágenes al aplicarse el uso de cámaras, videocámaras y a cualquier medio técnico análogo, que capte y/o registre imágenes. Ello con el ánimo de establecer un equilibrio entre el derecho de seguridad y el derecho a la protección de datos personales. Es de considera también ciertos aspectos dentro de la sociedad de la información que tiendan a regular el fijación de las imágenes personales bajo los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad en el manejo y salvaguarda de la protección de datos personales en posesión de los particulares.[132]

Por tanto aquellas personas físicas o morales ya sean de carácter público o privado que justifican la captación de imágenes de personas mediante la modalidad de videovigilancia en aras de proteger su seguridad privada, seguridad nacional o la conservación de su patrimonio siempre y cuando se actualicen las siguientes circunstancias:

1.- Exista grabación, captación, transmisión, conservación, o almacenamiento de imágenes, incluida su reproducción o emisión en tiempo real o un tratamiento que resulte de los datos personales relacionados con aquélla.

2.- Tales actividades se refieran a datos de personas identificadas o identificables.

---

[132] Los principios referidos se encuentran contemplados en el artículo 6, Capítulo Segundo, De los principios de Protección de Datos Personales plasmados en la Ley de Protección de Datos Personales en Posesión de los Particulares en México, publicada el día Lunes 5 de Julio de 2010 en el Diario Oficial de la Federación, Primera Sección.

Por tanto aquellos sujetos que realizan dichas actividades se encuentran obligados a implementar controles sobre el almacenamiento, uso y divulgación de la información de las personas, ello con la finalidad de evitar posibles intromisiones de terceros a su vida privada en los cuales puedan afectar su intimidad o en algunos casos que en algún momento se puede traducir en un daño moral.[133]

Cabe destacar que pueden existir ciertas excepciones sobre los puntos ya señalados, cuando se realice una captación de imágenes de personas derivado de un uso domestico como puede ser la fijación de imágenes de un viaje turístico.

Ahora bien de lo antes expuesto se deben establecer una serie de directrices para el tratamiento y captación de imágenes de las cuales mencionaremos algunas:

1.- Debe justificarse plenamente la finalidad perseguida en la obtención de imágenes de personas como ya se expuso con anterioridad.

2.- Es obligatorio que se informe mediante un aviso o señalamiento que se está realizando una captación de imágenes.

3.- En cualquier caso el uso de sistemas de videovigilancia deberá ser respetuoso con los derechos de las personas y el resto de los distintos ordenamientos jurídicos como la Ley Federal del Derecho de Autor, Ley de Propiedad Industrial o la Ley General de Salud.

4.- Las imágenes se conservarán por el tiempo imprescindible para la satisfacción de la finalidad para la que se recabaron, es decir debe contemplarse el bloqueo conforme a lo dispuesto en el artículo 3 Fracción III de la LPDPPP.[134]

---

133 Álvarez Larrondo Federico Manuel, Ghersi Carlos Coordinador, *Los Nuevos Daños Soluciones Modernas de Reparación*, Editorial Hammurabi SRL, Buenos Aires 2000, p. 74

134 Se refiere la Ley de Protección de Datos Personales en Posesión de los Particulares publicada en el Diario Oficial de la Federación el 05 de Julio de 2010.

5.- En todo momento se podrá ejercitar los derechos ARCO por parte de los titulares de los datos. Estos consisten de acuerdo a lo establecido en la Ley de Protección de Datos Personales en Posesión de los Particulares en:

5.1. Acceso.- Siendo el derecho que le asiste al titular de los datos de acceder a su propia información incluyendo su propia imagen en los que a partir de que forman parte de una base de datos, ya sea en papel o algún soporte electrónico.

5.2. Rectificación.- Este derecho consiste en que el titular de los datos tiene la facultad de realizar una modificación de sus datos personales que se encuentren en una base de datos cuando sean incorrectos o incompletos.

5.3. Cancelación.- Este derecho consiste en la potestad que tiene el titular de los derechos para efecto de que sean eliminados en las bases de datos.

5.4. Oposición.- El titular de los datos puede ejercer este derecho en contra de un tercero que cuenta con datos personales suyos en una base de datos obtenidos sin su consentimiento.

Para efectos de comprender lo aquí expuesto y haciendo énfasis en el derecho de cancelación de todas las imágenes captadas por un sistema de videovigilancia respecto del titular de datos personales, es de considerar la resolución R/00294/2008 emitida por la Agencia Española de Protección de Datos en la que se ejerció el derecho de cancelación de todas sus imágenes captadas por las videocámaras instaladas en la Oficina de correos específicamente de su Centro Operativo de Seguridad. En la resolución aludida se obliga a dicho ente para efectos de que elimine todas las imágenes personales de quien ejerce dicho derecho.[135]

[135] RESOLUCIÓN Nº.: R/00294/2008 de fecha 02 de Abril de 2008 emitida por el Director de la Agencia Española de Protección de Datos consultada el día 22 de Enero de 2013 en el siguiente sitio electrónico http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2008/common/pdfs/TD-008232007_Resolucion-de-fecha-02-04-2008_Art-ii-culo-16-LOPD.pdf

En otro orden de ideas debemos considerar los distintos campos de aplicación de la videovigilancia como pueden ser las implementadas por empresas de seguridad pública o privada, accesos a edificios, salas de juego, entidades financieras, cámaras con acceso a la vía pública, cámaras conectadas a internet,[136] cámaras instaladas en estancias infantiles, espacios públicos de uso privado, videocámaras de cuerpos de seguridad, videocámaras de control de tráfico y vialidades, cámaras en eventos deportivos, espectáculos, prevención de emergencias y riesgos naturales, trabajos de inteligencia por parte de distintas autoridades, fines laborales, autotransporte privado entre otros.

En algunos países como es el caso de España se establecen ciertas reglas respecto el proceso de captación, almacenamiento, reproducción hasta su cancelación de imágenes. Es por ello que el responsable del tratamiento de las imágenes que son videograbadas deberá considerar en todo momento los siguientes aspectos:[137]

a) Debe existir una relación de proporcionalidad entre la finalidad perseguida y el modo en el que se traten los datos.

b) Debe informarse sobre la captación y/o grabación de las imágenes.

c) El uso de instalaciones de cámaras o videocámaras sólo es admisible cuando no exista un medio menos invasivo.

d) Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos.

---

136 En este sentido podemos mencionar que el almacenamiento de imágenes derivadas de la videovigilancia se denomina el "cloud computing" o computación en la nube siendo este definido como un nuevo esquema de prestación de servicios de tecnologías de la información que permiten el acceso a una gama de servicios uniformes sobre la plataforma de un entorno virtual.

137 Guía de Videovigilancia emitida por la Agencia Española de Protección de Datos consultada el día 22 de Enero de 2013 en http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf

e) Podrían tomarse imágenes parciales y limitadas de vías públicas cuando resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas.

f) En cualquier caso el uso de sistemas de videovigilancia deberá ser respetuoso con los derechos de las personas y el resto del cualquier ordenamiento jurídico.

g) Las imágenes se conservarán por el tiempo imprescindible para la satisfacción de la finalidad para la que se recabaron.

5.2. Disposiciones jurídicas de la videovigilancia en México

Respecto del uso de tecnologías de videovigilancia en algunas entidades federativas podemos mencionar lo que el Distrito Federal dispone de acuerdo a la Ley que regula el uso de tecnologías para la seguridad pública en el Distrito Federal la cual fue publicada en la Gaceta Oficial del Distrito Federal el 27 de Octubre de 2008. Esta regula la instalación de los equipos de videovigilancia de acuerdo a las siguientes justificaciones y criterios:

a) La videovigilancia deberá de implementarse en los lugares en los que se contribuya a prevenir y combatir conductas ilícitas garantizando el orden y la tranquilidad de la ciudadanía.

b) Se establece la prohibición de colocar equipos y sistemas tecnológicos en el interior de domicilios particulares o aquellos que se instalen en cualquier lugar con la finalidad de obtener información de tipo personal o familiar.

Ahora bien los criterios establecidos por las autoridades para establecer la instalación de sistemas de videovigilancia son los siguientes:

1.- Lugares en donde se registren los delitos de mayor impacto.

2.- Zonas con alto índice delictivo.

3.- Cruces y avenidas de transito abundante y peligroso.

4.- Lugares y Zonas peligrosas.

5.- Lugares en donde exista un alto grado de concurrencia cívica.

6.- Aquellos lugares que por su naturaleza se puedan ocasionar riesgos o alertar sobre algún fenómeno de pueda causar daño a la población.

Es de considerar que la disposición aludida establece el principio de licitud que proviene de la información que se obtenga mediante la videovigilancia cuando provenga de intervenciones de comunicaciones privadas no autorizadas conforme a la Ley. Ahora bien se considera ilícitas aquellas videograbaciones que sean susceptibles de clasificarse, analizarse, difundirse o distribuir sin apegarse a la Ley. Por último y para efectos de lo aquí expuesto también se consideran videograbaciones ilícitas cuando se obtengan del interior de un domicilio o violente el derecho a la vida privada de las personas.

Otras disposiciones normativa aplicable a la videovigilancia es la Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen en el Distrito Federal,[138] la cual para efectos del objeto de estudio del presente capitulo cabe mencionar lo que dispone su artículo 7 Fracción V, mismo que textualmente dispone lo siguiente:

> "*El ejercicio del derecho de personalidades una facultad que tienen los individuos para no ser molestados, por persona alguna, en el núcleo esencial de las actividades que legítimamente deciden mantener fuera del conocimiento público, para oponerse a la reproducción identificable de sus rasgos*

[138] Disposición normativa publicada en la Gaceta Oficial del Distrito Federal el día 19 de mayo de 2006.

físicos sobre cualquier soporte material sin su consentimiento y el respeto a la valoración que las personas hacen de la personalidad ético-social que se identifican con la buena reputación y la fama."

Es oportuno mencionar también lo dispuesto en el artículo 21 de la citada Ley, en cuanto a excepciones del derecho a la propia imagen,[139] las cuales consisten en lo siguiente:

I. Su captación, reproducción o publicación por cualquier medio, cuando se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público que sean de interés público.

II. La utilización de la caricatura de dichas personas, de acuerdo con el uso social.

III. La información gráfica sobre un suceso o acontecimiento público cuando la imagen de una persona determinada aparezca como meramente accesoria.

El estado de Colima cuenta con una Ley de Videovigilancia[140] la cual tiene por objeto regular la utilización de la videovigilancia, ya sea por las Instituciones de Seguridad Pública Estatales, Municipales y/o los prestadores de Servicios de Seguridad Privada. Dichas acciones se realizan a través de videocámaras para captar y grabar imágenes o sonidos en lugares públicos sean abiertos o cerrados y su posterior tratamiento, incluyendo también espacios privados destacando los siguientes aspectos en cuanto a justificación y salvaguarda de la propia imagen:

a) *La utilización de grabaciones estará presidida por el principio de proporcionalidad, en su doble versión de idoneidad y de intervención mínima;*

b) *La idoneidad determina que sólo podrá emplearse la grabación cuando resulte adecuado, en una situación concreta, en referencia a cierta periodicidad de hechos delictivos, para la seguridad ciudadana, de conformidad con lo dispuesto en esta Ley;*

139 La imagen es la reproducción identificable de los rasgos físicos de una persona sobre cualquier soporte material.

140 DECRETO No. 618 en el que se aprueba la ley que regula la video vigilancia en el estado de Colima consultado en el Periódico Oficial del Estado de Colima Tomo 94, Col., Sábado 22 de Agosto del año 2009; Núm. 38; pág. 2.

c) La intervención mínima exige la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la grabación al derecho a la intimidad de las personas, al honor y a la propia imagen; y

d) No se podrá utilizar el sistema de video vigilancia para tomar imágenes y sonidos del interior de las viviendas, ni de sus vestíbulos, salvo consentimiento del titular o autorización judicial, cuando se afecte la intimidad de las personas.

Otra entidad federativa que tiene normada la videovigilancia es Aguascalientes,[141] la cual principalmente regula la captación de imágenes con o sin sonido por los cuerpos de seguridad pública estatal o municipales o de seguridad privada. Cabe destacar que su sistema opera bajo el principio de intervención mínima considerando la ponderación, en cada caso, entre la finalidad pretendida y la posible afectación por la utilización de la videocámara al derecho a la intimidad de las personas, al honor y a la propia imagen. La videograbación en dicho estado opera bajo el principio de respecto a los derechos fundamentales, como se establece en su artículo 15 mismo que a la letra dice:

"Queda prohibida la instalación fija de videocámaras en instalaciones y lugares en los que se vulneren los derechos fundamentales de alguna persona."

Otro aspecto a considerar por parte de la citada ley es lo concerniente a lo dispuesto en su Capítulo IX relativo al derecho de los particulares, destacando lo que en especie señala su artículo 32, el cual se transcribe:

"*Toda persona tiene derecho a que se le informe en que lugares se realizan actividades de Videovigilancia y que autoridad o prestador de servicio de Seguridad Privada las realiza, para tal efecto, se deberán colocar anuncios pictográficos que contengan la leyenda "ESTE LUGAR ES VIDEOVIGILADO", el nombre de la autoridad o prestador de servicio de Seguridad Privada que realiza dicha actividad, y en caso de realizar grabaciones, el término en que se destruirán así como indicar los derechos de acceso, rectificación y oposición que se pueden ejercer en términos de esta Ley*."

[141] Ley publicada en la Primera Sección del Periódico Oficial del Estado de Aguascalientes, el lunes 22 de junio de 2009.

Existen otras disposiciones normativas de carácter federal que protegen la propia imagen y que pudiesen ser ejercidas por los titulares de los datos frente a la captación de imágenes por medio de sistemas de videovigilancia, como es el caso de lo que dispone la Ley Federal del Derecho de Autor en su artículo 87, mismo que señala lo siguiente:

> *"Artículo 87.- El retrato de una persona sólo puede ser usado o publicado, con su consentimiento expreso, o bien con el de sus representantes o los titulares de los derechos correspondientes. La autorización de usar o publicar el retrato podrá revocarse por quien la otorgó quién, en su caso, responderá por los daños y perjuicios que pudiera ocasionar dicha revocación.*
>
> *Cuando a cambio de una remuneración, una persona se dejare retratar, se presume que ha otorgado el consentimiento a que se refiere el párrafo anterior y no tendrá derecho a revocarlo, siempre que se utilice en los términos y para los fines pactados.*
>
> *No será necesario el consentimiento a que se refiere este artículo cuando se trate del retrato de una persona que forme parte menor de un conjunto o la fotografía sea tomada en un lugar público y con fines informativos o periodísticos."*

Otra disposición que aplica a la protección a la propia imagen es la establecida en la Ley de Propiedad Industrial, en lo que respecta al uso del retrato de las personas en las marcas, mismo que señala lo siguiente en su artículo 90:

> *"No serán registrables como marca:*
>
> *XII.- Los nombres, seudónimos, firmas y retratos de personas, sin consentimiento de los interesados o, si han fallecido, en su orden, del cónyuge, parientes consanguíneos en línea recta y por adopción, y colaterales, ambos hasta el cuarto grado*;"

Los citados cuerpos normativos constituyen en esencia la regulación en México de la Videovigilancia y la protección de datos personales; siendo que la mayoría justifica la capitación de imágenes considerando el respeto a la intimidad, el honor y a la propia imagen de las personas.

Conclusión Capitular

La imagen de toda persona es única y esta tiene la facultad de autodeterminación en cuanto a la captación, reproducción y publicación de su propia imagen. Es por ello que todos los ciudadanos debemos considerar que en lugares tanto públicos como privados se han instalado sistemas de videograbación que en algunas ocasiones desconocen que su imagen está siendo captada y resguardada en un centro de datos como lo es en la video vigilancia. La justificación inicial de dicha actividad parte de la implementación de un mecanismo que se usa para garantizar la seguridad patrimonial o la integridad de las personas físicas y morales y en otras ocasiones para el cumplimiento de sus obligaciones como es el caso de las observaciones de un reglamento de tránsito en una institución bancaria.

La videovigilancia debe realizarse de acuerdo a las disposiciones que la Ley señale de lo contrario se podría estar violando un derecho constitucional en materia de protección de datos personales. Cabe mencionar que los sujetos que realizan las actividades de video vigilancia deben implementar controles sobre su almacenamiento, uso y divulgación ello con la finalidad de evitar intromisiones de terceros y en su momento este cause daño moral. Cabe destacar lo que en especie señala la Ley que regula la videovigilancia en el Distrito Federal, ya que esta contempla que la videovigilancia solo podrá utilizarse e implementarse en lugares donde ayude a contribuir y disminuir las conductas ilícitas y hechos delictivos garantizando así la seguridad y tranquilidad de los ciudadanos.

C O N C L U S I O N E S

PRIMERA: A lo largo de la presente investigación se desarrollaron ciertos aspectos fundamentales respecto de las facultades que tenemos las personas físicas frente a aquellos particulares que recaban datos personales especialmente aquellos relativos a la tutela efectiva del acceso, rectificación, cancelación y oposición de la información personal de los sujetos identificables. Para ello se examinaron y explicaron las etapas formales que rigen los procedimientos para ejercer los citados derechos ya sea mediante la identificación de los sujetos que intervienen, tipología de las resoluciones y recursos administrativos que pueden interponerse cuando no se satisfaga el interés jurídico del titular del derecho. Por lo tanto dicha información será de suma utilidad para la compresión que tenemos los titulares de datos personales respecto del marco procedimental que los regula.

Por lo que respecta a su parte especial después haber realizado el minucioso análisis de cada uno de los derechos de acceso, rectificación, cancelación y oposición; así como del desarrollo del procedimiento específico para ejercer por parte de las personas considerando cada uno de los derechos aquí expuesto de acuerdo a la naturaleza y a las características propias de cada uno de ellos. Algunas de estas pueden por una causal de negativa de los citados derechos o la existencia de una excepción por parte de los sujetos regulados. Es de considerar también la exposición de algunas resoluciones significativas que ayudan a comprender a cabalidad el bien jurídico que cada uno de estos derechos tutelan en materia de protección de datos personales. Por lo tanto la presente investigación coadyuva como una herramienta eficaz en la actuación en el ejercicio efectivo de los derechos ARCO.

Adicionalmente, se explicaron y diferenciaron las figuras del derecho de cancelación y revocación del consentimiento en materia de protección de datos, ya que de manera constate causan una confusión y se consideran como sinónimos, lo que conlleva a una correcta compresión y ejercicio de dichas figuras frente a los sujetos regulados.

Otro aportación de la presente investigación fue la relativa al análisis de la figura del tratamiento de datos personales en decisiones sin intervención humana valorativa establecido en el reglamento de la LFPDPPP y la cual resulta ilegal toda vez ya que la misma no se encuentran regulada en la citada ley. No obstante se determino la importancia que dicha figura de acuerdo al paralelismo que se realizo con la figura análoga establecida en la legislación española.

SEGUNDA: En lo que respecta al minucioso análisis efectuado de manera sistemática del procedimiento de verificación en materia de protección de datos personales, podemos afirmar que servirá como un material de consulta y actuación, el cual estará disponible en los acervos bibliográficos de la División de Estudio de Posgrado de la Facultad de Derecho y Ciencias Sociales. Así también se propondrá su difusión en otras universidades y autoridades en la materia. Lo anterior será sumamente útil para aquellos sujetos regulados que desconocen las facultades y procedimientos que el Instituto Federal de Acceso a la Información y Protección de Datos Personales puede realizar dentro de las facultades que le confiere su reglamento interior, sobre todo en lo que respecta a los elementos sustantivos que pueden ser objeto de revisión en un procedimiento de verificación de datos personales, aunado a que podrán implementar las directrices y medidas de seguridad que en materia de protección exige la normatividad.

TERCERA: El procedimiento administrativo sancionador expuesto es una figura jurídica novedosa en México. Por ende son pocos los pronunciamientos que se han generado por parte de la autoridad reguladora. Sin embargo a raíz del estudio aquí expuesto los sujetos regulados, juristas y todo aquel interesado en conocer las fases de dicho procedimiento, en correlación con las figuras jurídicas aplicables tales como la caducidad, la prescripción, apercibimiento y otras consideraciones como la ponderación del beneficio obtenido por el infractor como un criterio para la imposición de las sanciones en materia de protección de datos personales. Se afirma que el análisis servirá como una guía detallada para gestión, trámite y resolución de las partes que intervienen en acciones u omisiones en materia de protección de datos personales en cuanto a la aplicación de una sanción administrativa. Cabe hacer mención que para facilitar los procedimientos de tutela efectiva de derechos, procedimiento de verificación y procedimientos administrativo sancionador, se adicionaron

formularios y formatos que coadyuvan con el ejercicio más eficaz de los mismos, ya sea tanto para sujetos regulados y los titulares de los datos personales. Por tal razón el presente manual técnico-jurídico además de proporcionar la información sustantiva en materia de datos personales, facilita y fomenta la cultura de respeto a la privacidad e intimidad de los ciudadanos y como un instrumento factico de tutela de unos de los derechos de las personalidad que salvaguarda.

CUARTA: La figura de la videovigilancia en aras de proteger la seguridad de las personas o su patrimonio puede en un momento dado invadir el derecho a la propia imagen. En razón de que las imágenes captadas por videocámaras hacen identificable a las persona de acuerdo a los rasgos fisonómicos. Ahora bien es importante establecer un marco normativo que obligue a que las imágenes de las personas sean tratadas de manera licita, con fines estrictamente determinados y legítimos, siendo manejados de una forma pertinente, debiendo considerar en algún momento la ponderación de intereses públicos, la necesidad del cumplimiento de relaciones contractuales o la posible afectación de un interés mayor jurídicamente tutelado.

Es importante que el titulares de los derechos de la propia imagen sea previamente informado que su imagen está siendo captada por sistema de video vigilancia, para que en su momento puede ejercer su derecho subjetivo en cuanto al acceso, rectificación y cancelación de datos.

Cabe establecer la incipiente regulación respecto de la seguridad en las operaciones del tratamiento de imágenes, por lo que resulta necesario establecer controles previos ya sea técnicos y legales para evitar riesgos en probables violaciones de derechos y libertades de los interesados.

Dentro de las disposiciones importantes a considerar es el almacenamiento y transferencia registrados en la bases de datos que contienen imágenes de personas, los cuales son enajenados de manera ilícita o son utilizados indebidamente en redes sociales o portales de internet sin consentimiento de sus titulares. Cabe hacer la aclaración que en otros

casos la imágenes de personas captados por sistemas de videovigilancia han ayudado a identificar plenamente a los autores materiales de ciertos ilícitos como es el robo a instituciones bancarias, asalto a tiendas de autoservicio, o la identificación plena de homicidas.

FORMATOS

1.-EJERCICIO DEL DERECHO DE ACCESO DE DATOS PERSONALES.

2.-EJERCICIO DEL DERECHO DE RECTIFICACIÓN.

3.-EJERCICIO DEL DERECHO DE CANCELACIÓN

4.-EJERCICIO DEL DERECHO DE OPOSICIÓN

5.-CARTA DE CONTESTACIÓN AL DERECHO DE ACCESO EXISTIENDO INFORMACIÓN.

6.-CARTA DE CONTESTACIÓN AL DERECHO DE ACCESO SIN EXISTIR INFORMACIÓN.

7.-CARTA DENEGANDO EL ACCESO, RECTIFICACIÓN O CANCELACIÓN CUANDO ES SOLICITADA POR REPRESENTANTES.

8.-CARTA DENEGANDO EL ACCESO, RECTIFICACIÓN O CANCELACIÓN PROVISIONALMENTE PARA SUBSANACIÓN DE DEFECTOS.

9.-CARTA DE COMUNICADO EN EL NO PROCEDE LA RECTIFICACIÓN O CANCELACIÓN.

10.-MODELO DE DENUNCIA ANTE EL IFAI POR INOBSERVANCIA A LA TUTELA EFECTIVA DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES.

11.-MODELO DE AVISO DE PRIVACIDAD.

12.-AVISO DE PRIVACIDAD CON CESIÓN DE DATOS.

13.-ACUERDO DE CONFIDENCIALIDAD.

14.-CONTRATO DE CONFIDENCIALIDAD.

1.-EJERCICIO DEL DERECHO DE ACCESO DE DATOS PERSONALES

Nombre de la empresa_____, en cumplimiento de las obligaciones recogidas en la normativa de protección de carácter personal, reconoce y garantiza el derecho de acceso a sus datos de carácter personal, que fueron incorporados en los archivos de _____ para el mejor desarrollo de la relación comercial.

Datos del solicitante:

Sr / Sra._____mayor de edad con domicilio en la calle _____ con número de la colonia_____ en la ciudad de _____ C.P. ____, por medio del presente escrito manifiesta se deseo de ejercer su derecho de acceso, de conformidad con lo dispuesto en el artículo___ de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y lo dispuesto en el artículo ___ de su reglamento.

Solicita:

1.- Obtener gratuitamente información de sus datos de carácter personal sometidos a su tratamiento.

2.- Que si la solicitud del derecho de acceso fuese estimada, se remita por correo la información a la dirección abajo indicada. Mediante medio inteligible.

Para acreditar su identidad y, con ello, garantizar su seguridad y la del tratamiento de sus datos, es necesario que junto a esa solicitud acompañe una fotocopia de un documento de identidad.

La dirección a la que deberá dirigir la presente solicitud para el ejercicio de este derecho es la siguiente:_____

Firma del solicitante.

En la ciudad de _____ a_____ de_____ de 2014.

2.-EJERCICIO DEL DERECHO DE RECTIFICACIÓN

XXX (nombre de la empresa), en cumplimiento de las obligaciones establecidas en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, la cual reconoce y garantiza el derecho de rectificación de sus datos de carácter personal, que fueron incorporados a los ficheros de XXX para el (objeto de recabar información)

Datos del Solicitante:

Sr / Sra._____mayor de edad con domicilio en la calle _____ con número de la colonia_____ en la ciudad de _____ C.P. ____, por medio del presente escrito manifiesta se deseo de ejercer su derecho de acceso, de conformidad con lo dispuesto en el artículo___ de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y lo dispuesto en el artículo ___ de su reglamento.

Que XXXX modificar sus datos personales respecto de:

1.-……..
2.-…….
3.-…….

Para acreditar su identidad y con ello, garantizar su seguridad y el tratamiento de sus datos, es necesario que junto con esta solicitud acompañe una fotocopia del documento que acredita su identidad.

La dirección a la que deberá de dirigirse la presente solicitud para el ejercicio de esta derecho es la siguiente:

Firma del solicitante:

En la ciudad de _____ a_____ de_____2014.

3.-EJERCICIO DEL DERECHO DE CANCELACIÓN

Nombre de la empresa_____, en cumplimiento de las obligaciones establecidas en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, la cual reconoce y garantiza el derecho de cancelación de sus datos de carácter personal, que fueron incorporados a las bases de datos y/o archivos de _____ para el (objeto de recabar información)

Datos del Solicitante:

Sr / Sra._____mayor de edad con domicilio en la calle _____ con número de la colonia_____ en la ciudad de _____ C.P. ____, por medio del presente escrito manifiesta se deseo de ejercer su derecho de acceso, de conformidad con lo dispuesto en el artículo___ de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y lo dispuesto en el artículo ___ de su reglamento.

Que _____ cancele de sus archivos los siguientes datos personales correspondientes a mi persona respecto de:

1.-……..
2.-…….
3.-…….

Advertencia: Cuando la cancelación lo sea todos de datos personales o, al menos, de aquellos necesarios para la relación entre usted y _____ se pueda seguir desarrollando, se procederá a la baja en el servicio _____ o en la relación de _____.

Para acreditar su identidad y con ello, garantizar su seguridad y el tratamiento de sus datos, es necesario que junto con esta solicitud acompañe una fotocopia del documento que acredita su identidad.

La dirección a la que deberá de dirigirse la presente solicitud para el ejercicio de esta derecho es la siguiente:

Firma del solicitante:

En la ciudad de_____a_____de_____2014.

4.-EJERCICIO DEL DERECHO DE OPOSICIÓN

Datos del responsable de los datos:
Nombre / razón social: _____

Dirección de la Oficina / Servicio ante el que se ejercita el derecho de oposición: Calle_____ No_____ Código Postal _____ Localidad _____Estado _____.

DATOS DEL INTERESADO O REPRESENTANTE LEGAL

Sr / Sra._____mayor de edad con domicilio en la calle _____ con número de la colonia_____ en la ciudad de _____ C.P. ____, por medio del presente escrito manifiesta se deseo de ejercer su derecho de acceso, de conformidad con lo dispuesto en el artículo___ de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y lo dispuesto en el artículo ___ de su reglamento.

VENGO A EXPONER LO SIGUIENTE:

(describir la situación en la que se produce el tratamiento de sus datos personales y enumerar los motivos por los que se opone al mismo)

Para acreditar la situación descrita, acompaño una copia de los siguientes documentos:

1.-
2.-
3.-

(enumerar los documentos que adjunta con esta solicitud para acreditar la situación que ha descrito)

SOLICITO,

Que sea atendido mi ejercicio del derecho de oposición en los términos anteriormente expuestos.

En _____a_____de_____de 2014.

Firmado:

5.-CARTA DE CONTESTACIÓN AL DERECHO DE ACCESO EXISTIENDO INFORMACIÓN

Referencia:_____

SR. O SRA.
PRESENTE:

Se ha recibido en nuestras oficinas su petición de fecha_____, adjuntando la siguiente documentación….., y mediante la cual ejerce el derecho de acceso a sus datos que estén registrados en nuestros archivos y conforme a la normativa vigente sobre protección de datos personales en posesión de los particulares, se hace la siguiente notificación:

(PONER DATOS)

Le comunicamos que, si usted considera que estos datos son incompletos o inexactos, puede solicitar el derecho de rectificación o en su caso el de cancelación, acompañando a su petición los documentos que justifiquen la rectificación o cancelación.

Le comunicamos también que sus datos tienen como origen (DESCRIBIR EL ORIGEN DE LOS DATOS) y que no han sido comunicados o cedidos a ninguna persona física o moral.

Igualmente se le informa que para el ejercicio de sus derechos podrá obtener la tutela del Instituto Federal de Acceso a la Información y Protección de Datos Personales, dirigiendo su reclamación a (domicilio del IFAI.

Firmado

Datos de la empresa.

6.-CARTA DE CONTESTACIÓN AL DERECHO DE ACCESO SIN EXISTIR INFORMACIÓN

Referencia:_____

Sr. O Sra.
PRESENTE:

Se ha recibido en nuestras oficinas su carta de fecha____, adjuntando la siguiente documentación_____, y mediante la cual ejerce el derecho de acceso a sus datos que estén registrados en nuestros archivos y, conforme a la normativa vigente sobre la protección de datos en posesión de los particulares, le notificamos que en nuestros archivos no se encuentra ningún dato de carácter personal referente a usted.

Igualmente se le informa que para el ejercicio de sus derechos podrá obtener la tutela del Instituto Federal de Acceso a la Información y Protección de Datos Personales, dirigiendo su reclamación a (domicilio del IFAI.

Firmado

Datos de la empresa.

7.-CARTA DENEGANDO EL ACCESO, RECTIFICACIÓN O CANCELACIÓN CUANDO ES SOLICITADA POR REPRESENTANTES

Referencia:_____

Sr. O Sra.

Se ha recibido en nuestras oficinas su petición de fecha_____; adjuntando la siguiente documentación _____, y mediante la cual solicita el acceso/rectificación/cancelación a los datos que se encuentran en nuestros archivos; queremos comunicarle que, de acuerdo con lo especificado en la normativa sobre protección de datos de carácter personal, se trata de un derecho personalísimo, por lo que, si su voluntad es ejercerlos, le solicitamos que nos envié un escrito, con su firma y fotocopia de una identificación oficial, expresando su voluntad al respecto, así como la justificación de la representación conferida.

Igualmente se le informa que para el ejercicio de sus derechos podrá obtener la tutela del Instituto Federal de Acceso a la Información y Protección de Datos Personales, dirigiendo su reclamación a (domicilio del IFAI).

Firmado

Datos de la empresa.

8.-CARTA DENEGANDO EL ACCESO, RECTIFICACIÓN O CANCELACIÓN PROVISIONALMENTE PARA SUBSANACIÓN DE DEFECTOS

Referencia: XXXX

Sr. O Sra.

Se ha recibido en nuestras oficinas su petición de fecha XXXXX; adjuntando la siguiente documentación XXXX, y mediante la cual solicita el acceso/rectificación/cancelación a los datos que se encuentran en nuestros archivos; queremos comunicarle que, de acuerdo con lo especificado en la normativa sobre protección de datos de carácter personal, su solicitud debe ser completada en los aspectos que a continuación se señalan:

-Nombre, apellidos del interesado.
-Fotocopia de identificación oficial.
-Nombre y apellidos de la persona que los represente, así como el documento que acredita la representación.
-Firma del interesado o representante de la solicitud.
-Documentos acreditativos de la petición que se formula:

-No identificar los datos que se quieren rectificar, o no acompañarlos de los documentos que acrediten la necesidad de la rectificación.

-No identificar los datos que se quieran cancelar, o no acompañarlos de los documentos que acrediten la necesidad de la rectificación.

- Otros

Igualmente se le informa que para el ejercicio de sus derechos podrá obtener la tutela del Instituto Federal de Acceso a la Información y Protección de Datos Personales, dirigiendo su reclamación a (domicilio del IFAI).

Firmado

Datos de la empresa.

9.-CARTA DE COMUNICADO EN EL QUE NO PROCEDE LA RECTIFICACIÓN O CANCELACIÓN.

Referencia:XXXX

Sr. O Sra.

Se ha recibido en nuestras oficinas su petición de fecha XXXXX; adjuntando la siguiente documentación XXXX, y mediante la cual solicita la rectificación/cancelación a los datos que se encuentran en nuestros archivos; queremos comunicarle que, de acuerdo con lo especificado en la normativa sobre protección de datos de carácter personal, no procede la solicitada rectificación o cancelación por los siguientes motivos:

(INDICAR MOTIVOS)

Igualmente se le informa que para el ejercicio de sus derechos podrá obtener la tutela del Instituto Federal de Acceso a la Información y Protección de Datos Personales, dirigiendo su reclamación a (domicilio del IFAI).

Firmado

Datos de la empresa.

10.-MODELO DE DENUNCIA ANTE EL IFAI POR INOBSERVANCIA A LA TUTELA EFECTIVA DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES

DATOS DEL AFECTADO

C……..mayor de edad, con domicilio a efectos de notificaciones en……., calle……, número…..., de la cuidad de ……, con Código Postal…., con credencial para votar emitida por el Instituto Federal Electoral número……., cuya copia se adjunta como documento número….

DATOS DEL PRESUNTO RESPONSABLE

Nombre/Razón Social……Dirección/Oficina/Servicio……..en ……..,calle…….., número…….Código Postal de la ciudad de …….. , con numero de credencial para votar……

MANIFIESTO

Que con fundamento en lo dispuesto en el artículo ____ de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, vengo a poner en conocimiento del Instituto Federal de Acceso a la Información Pública y Protección de Datos los siguientes hechos que se justifican con la documentación anexa al presente escrito:

HECHOS

Primero:…..(explicar los hechos, razones y petición en que se concreta la solicitud) cuya justificación se acompaña como documento numero….

Segundo…(explicitar los hechos, razones y petición en que se concreta la solicitud cuya justificación se acompaña como documento número…..

Tercero:….(explicitar los hechos, razones y petición en que se concreta la solicitud cuya justificación se acompaña como documento número…..

En virtud de cuanto antecede se

SOLICITA:

Que previas las comprobaciones que estime oportuno realizar, se dicte acuerdo de inicio de procedimiento sancionador, con el fin de evitar alguna presunta violación a la Ley Federal

de Protección de Datos Personales en Posesión de los Particulares, y se me notifique la resolución que recaiga.

En la ciudad de…….a……..de……2014

Firmado.

11.-MODELO DE AVISO DE PRIVACIDAD

Los datos personales recabados conforme a la previsto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en el presente aviso, serán incluidos en los archivos (denominación del archivo) y cuya titularidad pertenece (nombre de la entidad y dirección) en adelante responsable de los datos.

La finalidad de recabar datos de carácter personal es (indicar finalidades). En caso de negarse a comunicar los datos, podría ser imposible mantener la relación (administrativa, comercial o profesional) con usted.

En su calidad de titular de sus datos personales otorga su consentimiento y autorización al responsable del tratamiento de los datos para la inclusión de los mismos en los archivos en referencia. En cualquier caso podrá ejercitar sus derechos de acceso, rectificación, cancelación y oposición dirigiéndose a (nombre de la entidad) con dirección en (domicilio de la entidad) o bien y con carácter previo a tal actuación solicitarlas mediante los formatos impresos (o por correo electrónico) que el responsable del tratamiento de los datos dispone para tal efecto.

Por todo ello otorga su consentimiento para los efectos legales a que haya lugar.

12.-AVISO DE PRIVACIDAD CON CESIÓN DE DATOS

Los datos personales recabados conforme a la previsto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en el presente aviso, serán incluidos en los archivos (denominación del archivo) y cuya titularidad pertenece (nombre de la entidad y dirección) en adelante responsable de los datos.

Asimismo, el titular de los datos autoriza expresamente a ceder los mismos a las siguientes organizaciones: (listado de empresas u organizaciones), con la finalidad de que estas compañías puedan remitir, por cualquier medio, información sobre sus respectivos servicios, productos, ofertas o promociones especiales (incluir más u otras finalidades si fuere oportuno).

Para ello el Responsable de los datos cederá, con la finalidad indicada, los siguientes datos de carácter personal: (listado de datos cedidos), pudiendo usted en todo caso ejercitar los derechos que le asisten y que, a renglón seguido, se especifican.

La finalidad de esta recolección de datos de carácter personal es: (indicar la finalidad de la recogida). En caso de negarse a comunicar los datos, podría ser imposible mantener cualquier tipo de relación (administrativa, comercial o laboral) con usted.

Usted otorga como titular de los datos, su consentimiento y autorización al Responsable del Fichero para la inclusión de los mismos en el archivo detallado. Así mismo, declara estar informado de las condiciones y cesiones detalladas en la presente cláusula y, en cualquier caso, podrá ejercitar gratuitamente los derechos de acceso, rectificación, cancelación y oposición (siempre de acuerdo con los supuestos contemplados por la legislación vigente) dirigiéndose a (nombre de la entidad), con dirección (dirección), o bien y con carácter previo a tal actuación, solicitar con las mismas señas que le sean remitidos los impresos que el Responsable del tratamiento que dispone a tal efecto.

En caso de que se oponga a la cesión de sus datos en los términos previstos marque una cruz en esta casilla. En caso contrario, se entenderá que presta su consentimiento tácito a tal efecto.

13.-ACUERDO DE CONFIDENCIALIDAD

Por el presente documento, _____actuando en nombre y representación de la empresa_____en adelante denominada la Empresa, _____, con domicilio comercial en _____participante en el proyecto _____, en adelante PROYECTO,

MANIFIESTA:

• Que la EMPRESA se dedica a _____
• Que la EMPRESA dispone de información tecnológica referente al PROYECTO
• Que la EMPRESA está interesada en tener acceso a la información necesaria para llevar a cabo el PROYECTO

Por lo expuesto la EMPRESA,

SE COMPROMETE A:

PRIMERO.- A que toda la información de carácter confidencial suministrada y obtenida, NO sea facilitada a ninguna otra persona que no esté implicada en el proceso.

SEGUNDO.- A que la información de carácter confidencial obtenida en el proceso NO llegue a conocimiento de terceros por causas de negligencia, entendiéndose a tales efectos que el riesgo de pérdida casual, robo, etc. de dicha información, será responsabilidad de la EMPRESA.

TERCERO.- A que la información de carácter confidencial obtenida NO se utilice con fines distintos al del proyecto.

CUARTO.- A responder por el incumplimiento de las obligaciones asumidas en los compromisos anteriores, sin perjuicio, en su caso, de la responsabilidad penal de acuerdo con la legislación vigente.
En cualquier caso la EMPRESA, está obligada al cumplimiento de lo dispuesto en:

• La Ley Federal de Protección de Datos Personales en Posesión de los Particular, y sus disposiciones de desarrollo, y demás normativa vigente.

QUINTO.- En todo caso, la EMPRESA garantiza que el acceso a la información se limitará estrictamente a aquellos empleados de la misma que necesiten información para cumplir con los fines precisos en el PROYECTO y que éstos estarán obligados a guardar el secreto, a que obliga la Ley, de la información obtenida, extendiéndose el presente acuerdo a aquellas empresas subcontratadas y sus empleados, para la realización del PROYECTO.

SEXTO.- La duración de los compromisos asumidos en el presente documento comprenderá la completa duración del PROYECTO, y se prorrogará por un periodo de……..año/s a partir de la fecha de finalización del contrato, salvo que las partes expresamente autoricen su difusión.

Y para que así conste a los efectos oportunos se extiende por duplicado en el lugar y fecha indicados.

En ……,a…….de ……. de 2014.

Entidad

_____

Firma representante_____

14.-CONTRATO DE CONFIDENCIALIDAD

Al objeto de garantizar la confidencialidad del presente [Proyecto, colaboración entre las partes implicadas], se hace necesario la firma de un acuerdo que garantice unos niveles de confianza entre las partes. El documento se firmará una vez aceptado y firmado el (tipo: contrato, acuerdo,...] por ambas partes.

El contenido del acuerdo es el que figura a continuación.

Contenido

DE UNA PARTE: [nombre de la organización]y en su nombre y representación (con poder suficiente para ello) Sr. O Sra [nombre completo], en calidad de [cargo, administrador, apoderado,...]

DE OTRA PARTE: [nombre de la organización]. y en su nombre y representación (con poder suficiente para ello) Sr o Sra. [nombre completo], en calidad de [cargo, administrador, apoderado,...]
Reunidos en [lugar de la firma del contrato], a [día] de [Mes] de [Año]

EXPONEN LO SIGUIENTE:

I – Que las partes, anteriormente citadas, están interesadas en el desarrollo del presente contrato, para lo cual, aceptaron celebrar el presente Acuerdo de Confidencialidad con el fin de establecer el procedimiento que regirá la custodia y no transmisión a terceros de la información distribuida entre las partes, así como los derechos, responsabilidades y obligaciones inherentes en calidad de remitente, Propietario y «Destinatario» de la referida información.

II – Que las partes, en virtud de lo anteriormente expuesto, convinieron que el presente Acuerdo de Confidencialidad se rija por la normativa aplicable al efecto y, en especial por las siguientes.

CLÁUSULAS

PRIMERA - Definiciones
A los efectos del presente Acuerdo, los siguientes términos serán interpretados de acuerdo con las definiciones anexas a los mismos. Entendiéndose por:

- «Información propia»: tendrá tal consideración y a título meramente enunciativo y no limitativo, lo siguiente:

Descubrimientos, conceptos, ideas, conocimientos, técnicas, diseños, dibujos, borradores, diagramas, textos, modelos, muestras, bases de datos de cualquier tipo, aplicaciones, programas, marcas, logotipos, así como cualquier información de tipo técnico, industrial, financiero, publicitario, de carácter personal o comercial de cualquiera de las partes, esté o

no incluida en la solicitud de oferta presentada, independientemente de su formato de presentación o distribución, y aceptada por los «Destinatarios»

- «Fuente»: tendrá la consideración de tal, cualquiera de las partes cuando, dentro de los términos del presente acuerdo, sea ella la que suministre la Información Propia y/o cualquiera de los implicados (accionistas, directores, empleados, …) de la empresa o la organización.

- «Destinatarios»: tendrán la consideración de tales cualquiera de las partes cuando, dentro de los términos del presente Acuerdo, sea ellos quienes reciban la Información Propia de la otra parte.

SEGUNDA.- Información Propia.

Las partes acuerdan que cualquier información relativa a sus aspectos financieros, comerciales, técnicos, y/o industriales suministrada a la otra parte como consecuencia de la solicitud de Oferta para el desarrollo del presente proyecto objeto del contrato, o en su caso, de los acuerdos a los que se lleguen (con independencia de que tal transmisión sea oral, escrita, en soporte magnético o en cualquier otro mecanismo informático, gráfico, o de la naturaleza que sea) tendrá consideración de información confidencial y será tratada de acuerdo con lo establecido en el presente documento. Esa información, y sus copias y/o reproducciones tendrán la consideración de «Información propia» los efectos del presente acuerdo.

TERCERA.- Exclusión del Presente Acuerdo.

No se entenderá por «Información propia», ni recibirá tal tratamiento aquella información que:

I – Sea de conocimiento público en el momento de su notificación al «Destinatario» o después de producida la notificación alcance tal condición de pública, sin que para ello el «Destinatario» violentara lo establecido en el presente acuerdo, es decir, no fuera el «Destinatario» la causa o «Fuente» última de la divulgación de dicha información.

II – Pueda ser probado por el «Destinatario», de acuerdo con sus archivos, debidamente comprobados por la «Fuente», que estaba en posesión de la misma por medios legítimos sin que estuviese vigente en ese momento algún y anterior acuerdo de confidencialidad al suministro de dicha información por su legítimo creador.

III – Fuese divulgada masivamente sin limitación alguna por su legítimo creador.

IV – Fuese creada completa e independientemente por el «Destinatario», pudiendo este demostrar este extremo, de acuerdo con sus archivos, debidamente comprobados por la «Fuente».

CUARTA.- Custodia y no divulgación.

Las partes consideran confidencial la «Información propia» de la otra parte que le pudiera suministrar y acuerdan su guarda y custodia estricta, así como a su no divulgación o suministro, ni en todo ni en parte, a cualquier tercero sin el previo, expreso y escrito consentimiento de «Fuente». Tal consentimiento no será necesario cuando la obligación de suministrar o divulgar la «Información propia» de la «Fuente» por parte del «Destinatario» venga impuesta por Ley en vigor o Sentencia Judicial Firme.

Este Acuerdo no autoriza a ninguna de las partes a solicitar o exigir de la otra parte el suministro de información, y cualquier obtención de información de/o sobre la «Fuente» por parte del «Destinatario» será recibida por éste con el previo consentimiento de la misma.

QUINTA.- Soporte de la «Información propia».

Toda o parte de la «Información propia», papeles, libros, cuentas, grabaciones, listas de clientes y/o socios, programas de ordenador, procedimientos, documentos de todo tipo o tecnología en el que el suministro fuese hecho bajo la condición de «Información propia», con independencia del soporte que la contuviera, tendrá la clasificación de secreta, confidencial o restringida.

SEXTA.- Responsabilidad en la Custodia de la «Información propia».

La «Información propia» podrá ser dada a conocer por el «Destinatario» o sus directivos y/o sus empleados, sin perjuicio de que el «Destinatario» tome cuentas medidas sean necesarias para el exacto y fiel cumplimento del presente Acuerdo, debiendo necesariamente informar a unos y otros del carácter secreto, confidencial, o restringido de la información que da a conocer, así como da existencia del presente Acuerdo.
Así mismo, el «Destinatario» deberá dar a sus directivos y/o sus empleados, las directrices e instrucciones que considere oportunas y convenientes a los efectos de mantener el secreto, confidencial, o restringido de la información propia de la «Fuente». El «Destinatario» deberá advertir a todos sus directivos, empleados, etc., que de acuerdo con lo dispuesto en este acuerdo tengan acceso a la «Información propia», de las consecuencias y responsabilidades en las que el «Destinatario» puede incurrir por la infracción por parte de dichas personas, de lo dispuesto en este Acuerdo.

Sin perjuicio de lo anterior, la «Fuente» podrá pedir y recabar del «Destinatario», como condición previa al suministro de la «Información propia», una lista de los directivos y empleados que tendrán acceso a dicha información, lista que podrá ser restringida o reducida por la «Fuente».

Esta lista será firmada por cada uno de los directivos y empleados que figuren en ella, manifestando expresamente que conocen la existencia del presente Acuerdo y que actuarán de conformidad con lo previsto en él. Cualquier modificación de la lista de directivos y/o empleados a la que se hizo referencia anteriormente será comunicada de forma inmediata a la «Fuente», por escrito conteniendo los extremos indicados con anterioridad en este párrafo.

Sin perjuicio de lo previsto en los párrafos anteriores, cada parte será responsable tanto de la conducta dos sus directivos y/o empleados como de las consecuencias que de ella se pudieran derivarse de conformidad con lo previsto en el presente Acuerdo.

SÉPTIMA.- Responsabilidad en la custodia de la «Información propia».

El «Destinatario» será responsable de la custodia de la «Información propia» y cuantas copias pudiera tener de la misma suministrada por la «Fuente», en orden a su tratamiento, como secreta, confidencial o restringida, en el momento presente y futuro, salvo indicación explicita de la «Fuente».

Con el objeto de garantizar esta custodia, se deberá devolver la «Información propia» y cuantas copias pudiera tener de la misma suministrada por la «Fuente», a la terminación de las relaciones comerciales, o antes, si fuera requerido por la «Fuente» y respondiendo a los daños y perjuicios correspondientes, en el caso de incumplimiento de lo aquí dispuesto. (En aquellos casos en los que no fuera necesaria la devolución de la «Información propia» deberá eliminarse este párrafo)

OCTAVA.- Incumplimiento.
El incumplimiento de las obligaciones de confidencialidad plasmadas en este documento, por cualquiera de las partes, sus empleados o directivos, facultará a la otra a reclamar por la vía legal que estime más procedente, a la indemnización de los daños y perjuicios ocasionados, incluido el lucro cesante.

NOVENA.- Duración del Acuerdo de Confidencialidad.
Ambas partes acuerdan mantener el presente Acuerdo de Confidencialidad, aún después de terminar sus relaciones comerciales.

DECIMA.- Legislación Aplicable

El presente Acuerdo de Confidencialidad se regirá por la Legislación Mexicana, y cualquier disputa, controversia o conflicto en cuanto a la interpretación o ejecución del presente Acuerdo será sometido a la jurisdicción de los Tribunales de (Morelia), con exclusión de cualquier otro que pudiera corresponder a las partes, al que en este momento renuncian.

Y en prueba de esta conformidad, las partes firman o presente acuerdo, por duplicado y a un solo efecto, en el lugar y fecha.

FUENTES DE INFORMACIÓN

BIBLIOGRÁFICAS

ABA Catoira Ana, La Videovigilancia y la Garantía de los Derecho Individuales: su marco jurídico, Anuario de la Facultad de Derecho de la Facultad de la Coruña, España 2003, numero 7.

AGENCIA de Protección de Datos de la Comunidad de Madrid, Seguridad de Protección de Datos Personales, Ed. Agencia de Protección de Datos de Madrid, 2009 Madrid España. Págs. 558.

ALVAREZ Javier. Guía práctica sobre protección de datos. España. Lex Nova.2011.738 p.

ALVAREZ Larrondo Federico Manuel, Ghersi Carlos Coordinador, Los Nuevos Daños Soluciones Modernas de Reparación, Editorial Hammurabi SRL, Buenos Aires 2000

APARICIO Javier. Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal. Navarra. Editorial Aranzadi. 2000. 139 p.

ARENAS Mónica. El derecho fundamental a la protección de datos personales en Europa. Valencia. Tirant lo Blanch. 2006. 638 p.

BOIX REIG Javier, JAREÑO LEAL Ángeles y otros. La protección jurídica de la intimidad. España. Iustel Portal Derecho S.A. 2010. 663 p.

BUREAU VERITAS Formación. Ley de Protección de datos personales. Manual práctico para la protección de los datos personales de las personas físicas. España. Fundación CONFEMETAL. 2009. 295 p.

CASTAÑEDA, Alberto y BONADEO Rodrigo. Guía práctica de protección de datos de carácter personal. España. Ediciones Experiencia S.L., 2002. 300 p.

CONDE Concepción. La protección de datos personales. España. Editorial Dykinson S.L. 2005. 114 p.

COUDERT Fanny. Ejercicio de Derechos. En: ALMUZARA Cristina: Estudio práctico sobre la protección de datos de carácter personal. España. Editorial LEX NOVA S.A. 2005. 633 p.

COUSIDO Pilar. Derecho de la comunicación (vol. I): derecho de la comunicación I empresa. Editorial Colex. 2001. 302 p.

DAVARA Isabel. Hacia la estandarización de la protección de datos personales. España. La Ley. 2001. 607 p.

DAVARA Miguel Ángel. Manual de Protección de datos para abogados. España. Segunda Edición. Editorial Aranzadi S.A. 2008. 371 p.

DAVARA, Miguel Ángel. La protección de datos en Europa. Principios, derechos y procedimiento. Madrid. Asnef Equifax. 1998. 201 p.

DEL CASTILLO Isabel-Cecilia. Protección de datos: cuestiones constitucionales y administrativas, El derecho a saber y la obligación a callar. España. Editorial Aranzadi S.A. 2007. 740 p.

DEL PESO Emilio, RAMOS Miguel Ángel, DEL PESO Margarita. Nuevo Reglamento de Protección de Datos de Carácter Personal. España. Ediciones Díaz de Santos. 2008. 820 p.

DÍAZ-ARIAS José Manuel. Guía práctica sobre normativa de protección de datos y publicidad comercial. España. Ediciones Deusto. 2008. 358 p.

ECIJA. Factbook Protección de datos personales. El manual práctico para cumplir la Ley y el Reglamento LOPD. España. Tercera Edición Thomson Reuters. 2010. 1072 p.

ENÉRIZ Francisco Javier y BELTRÁN Juan Luis. La protección de los datos de carácter personal. Pamplona. Institución del Defensor del Pueblo de la Comunidad Floral de Navarra. 2012. 208 p.

FREIXAS Gabriel. La protección de los datos de carácter personal en el derecho español. España. Editorial Bosch S.A. 2001. 394 p.

GARCÍA Antonio. La protección de datos personales en México, Pretensión Regulatoria. México. Senado de la República. 2006. 343 p.

GUERRERO María del Carmen. El impacto de internet en el derecho fundamental a la protección de datos de carácter personal. España. Editorial Aranzadi, SA. 2006. 587 p.

GUTIERREZ Luis. Derecho de Rectificación y libertad de información. España. J.M Bosch Editor. 2003. 486 p.

HECKH Norman Coordinador. Memento Experto. Protección de Datos. España. Ediciones Francis Lefebvre. 2012. 342 p.

HOLVAST Jan, MADSEN Wayne y otros. The Global Encyclopaedia of Data Protection Regulatión. Netherlands. Kluwer Law Internacional. 1999-2001.

IBARRA Sánchez Ernesto, Videovigilancia Punto de Colisión entre Derechos Fundamentales, Seguridad y Protección de los Datos Personales en México, Acervo de la Biblioteca Jurídica de la UNAM, libro 6.

LACASTA Ramón y SANMARTÍ Ermengo. Auditoría de la protección de datos. España. Segunda Edición. Editorial Bosch S.A.. 2009 354 p.

LLACER María Rosa. Protección de datos personales en la sociedad de la información y vigilancia. España. La ley. 2011. 377 p.

LÓPEZ José. Actividad inspectora y procedimiento administrativo sancionador en materia de protección de datos personales. En: AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS. La potestad sancionadora de la Agencia Española de Protección de Datos. España. Editorial Aranzadi. 2008. 370 p.

LOPEZ-VIDRIERO TEJEDOR Iciar y SANTOS PASCUAL Efrén. Protección de Datos Personales, Manual práctico para empresas. España. Fundación CONFEMETAL. 2005. 257 p.

MARZO Ana y MACHO Alejandro. La auditoría de seguridad en la protección de datos de carácter personal. España. Segunda Edición. Ediciones Experiencia. 2009. 347 p.

MARZO Ana. Infracciones y sanciones. En: ALMUZARA Cristina: Estudio práctico sobre la protección de datos de carácter personal. España. Editorial LEX NOVA S.A. 2005. 633 p.

MUÑOZ José Félix y OLIVER-LALANA Daniel. Derecho y Cultura de Protección de Datos. Un estudio sobre la privacidad en Aragón. Madrid. Editorial DYKINSON S.L.. 2012. 314. P.

RALLO Artemi y ARROYO Luis. Robo de identidad y protección de datos. España. Editorial Aranzadi. S.A. 2010. 323 p.

RAMOS Miguel y Del Peso Emilio. La seguridad de los datos de carácter personal. 2ª Edición. España. Ediciones Díaz de Santos S.A. 2002. 245 p.

RUBIO Antonio María. Aspectos prácticos de la protección de datos de las personas físicas. España. M Bosch Editor. 2004. 574 p.

RUIZ Antonio. El tratamiento de los datos personales en los documentos de seguridad. España. Editorial Bosh S.A. 2008. 459 p.

RUIZ Antonio. Manual práctico de protección de datos. España. Editorial Bosch S.A. 2005. 232 p.

SALLA Xavi y ORTEGA Jorge. Actuaciones inspectoras en materia de protección de datos. España. Bosch Editor. 2008. 168 p.

SANCHEZ-CRESPO Antonio y PEREZ Elena. La Protección de Datos en los Centros de Enseñanza. España. Editorial Aranzadi S.A. 2007. 460 p.

SANTOS Daniel. Nociones generales de la Ley Orgánica de Protección de Datos. Madrid. Editorial Tecnos. 2005. 236 p.

SERRERA Pedro. Buenas Prácticas en Protección de datos. Fundación DINTEL. España. 2007. 449 p.

TASCÓN Rodrigo. El tratamiento por la empresa de datos personales de los trabajadores, Análisis del estado de la cuestión. España. Editorial Aranzadi. S.A. 2005.183 p.

TELLEZ Abel. Nuevas Tecnologías. Intimidad y Protección de datos. España. Edisofer S.A. 2001. 435 p.

TRONCOSO Antonio. La protección de datos personales… en busca del equilibrio. España. Tirant Lo Blanch. 2010. 1990 p.

VELAZQUEZ Rafael. Protección jurídica de datos personales automatizados. Madrid. Colex. 1993. 133 p.

VELEIRO Belen. Protección de datos de carácter personal y sociedad de la información. Madrid. Boletín Oficial del Estado. 2008. 672 p.

VERDAGUER Jordi y BERGAS María Antonia. 1000 Soluciones de Protección de Datos. España. Editorial CISS Wolters Kluwer España S.A. 2010. 651 p.

VERDAGUER Jordi y BERGAS María Antonia. TODO Protección de datos. España. Edición Contable Mercantil CISS. 2009. 874 p.

LEGISLACIÓN.

Constitución Política de los Estados Unidos Mexicanos

Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Diario Oficial de la Federación. México. 05 de Julio de 2010.

Ley Federal del Procedimiento Administrativo. Diario Oficial de la Federación. México. 9 de Abril de 2012.

Ley Federal del Derecho de Autor.

Ley de Propiedad Industrial

Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen en el Distrito Federal.

Ley de Video Vigilancia del estado de Aguascalientes

Ley de Video Vigilancia del estado de Colima.

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Diario Oficial de la Federación. México. 21 de Diciembre de 2011.

Reglamento Interior del Instituto Federal de Acceso a la Información y Protección de Datos. Diario Oficial de la Federación 29 de Octubre de 2012.

Reglamento de la Ley Federal de Derechos de Autor.

Reglamento de la Ley de Propiedad Industrial.

Ley Orgánica 2/1984 del 26 de Marzo, reguladora del Derecho de Rectificación en España.

Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal en España.

Propuesta del Reglamento del Parlamento Europeo y el Consejo relativo a la protección de personas físicas, en lo que respecta al tratamiento de protección de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos. Emitido por la Comisión Europea el 25 de Enero de 2012 en Bruselas.

ELECTRÓNICAS

Agencia Española de Protección de Datos. El derecho fundamental a la protección de datos: Guía para el ciudadano. [En línea]. España 2011. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/GUIA_CIUDADANO_OK.pdf

Listas Robinson de Exclusión Publicitaria. ¿Que es el servicio de listados Robinson?. [En línea]. España. 2013.Consultado el día 3 de Junio de 2013. Disponible en https://www.listarobinson.es/default.asp

CONDUSEF. Registro Público de usuarios que no desean información publicitaria de productos y servicios financieros (REUS). [En línea]. México. 2013. Consultado el día 9 de Junio de 2013. Disponible en: http://portalif.condusef.gob.mx/REUS/home.php

Comentarios al Anteproyecto del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Emitido por Guillermo Wolf en su carácter de vicepresidente ejecutivo y director general de la American Chamber/México. México. 2011. [En línea]. Consultado el día 9 de Junio de 2013. Disponible en: http://207.248.177.30/expediente/v99/_B001102856.pdf

Compartiendo Experiencias en la Implementación de la Ley de Protección de Datos. Verónica Ramírez, General Motors de México, S. de R.L. de C.V.. Chief Privacy Officer. Junio 28, 2011, consultado el 23 de Diciembre de 2013 en www.amcham.org.mx/cwt/external/.../webcontentpage.aspx?...

IFAI, Estudios sobre Sistemas de Datos Personales, Iniciación sobre modelos de bases de datos, México D.F. Septiembre de 2004, documento digital consultado en http://inicio.ifai.org.mx/_catalogs/masterpage/Documentos-de-Interes.aspx?a=m4.

IFAI, Metodología de Análisis de Riesgo BAA, Septiembre de 2013, documento electrónico consultado el día 27 de Diciembre de 2013 en http://inicio.ifai.org.mx/DocumentosdeInteres/Metodologia_de_Analisis_de_Riesgo_BAA_nuevo_aviso.pdf

Orden Jurídico Nacional consulta en línea en la siguiente dirección electrónica http://www.ordenjuridico.gob.mx/leyes.php

Procuraduría Federal del Consumidor. Registro Público Para Evitar Publicidad. [En línea]. México. 2013. Consultado el día 3 de Junio de 2013. Disponible en: http://rpc.profeco.gob.mx/rpc.jsp

Recomendaciones en materia de seguridad de datos personales emitido por el Pleno del Instituto Federal de Acceso a la Información y Protección de Datos, con fundamento en lo dispuesto por los artículos 19, 39, fracción IV de la Ley Federal de Protección de Datos

Personales en Posesión de los Particulares; 58 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; 15, fracciones I y XXI, 24, fracción III, y 30, fracción II del Reglamento Interior del Instituto Federal de Acceso a la Información y Protección de Datos publicado en el Diario Oficial de la Federación el 30 de Octubre de 2013, consultado vía electrónica en http://www.dof.gob.mx/nota_detalle.php?codigo=5320179&fecha=30/10/2013.

RESOLUCIONES

Estándares Internacionales sobre Protección de Datos Personales y Privacidad. Resolución de Madrid. Propuesta Conjunta para la Redacción de Estándares Internacionales para la Protección de la Privacidad en relación con el tratamiento de Datos de Carácter Personal .Conferencia Internacional de Autoridades de Protección de Datos y Privacidad 5 de Noviembre de 2009.

Resoluciones de Tutela de Derechos emitidos por la Agencia Española de Protección de Datos [En línea]. España. Agencia Española de Protección de Datos. Fecha de consulta 08 de Mayo de 2013. [En línea]. Disponible en http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/index-ides-idphp.php

Resoluciones de Tutela de Derechos emitidos por la Agencia Española de Protección de Datos [En línea]. España. Agencia Española de Protección de Datos. Fecha de consulta 14 de Mayo de 2013. [En línea]. Disponible en http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2011/common/pdfs/TD-01248-2011_Resolucion-de-fecha-30-12-2011_Art-ii-culo-34-RD-1720-b-2007.pdf

Resoluciones de Tutela de Derechos emitidos por la Agencia Española de Protección de Datos [En línea]. España. Agencia Española de Protección de Datos. Fecha de consulta 14 de Mayo de 2013. [En línea]. Disponible en http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2011/common/pdfs/TD-01075-2010_Resolucion-de-fecha-07-03-2011_Art-ii-culo-16-LOPD_Recurrida.pdf

Resoluciones de Tutela de Derechos emitidos por la Agencia Española de Protección de Datos [En línea]. España. Agencia Española de Protección de Datos. Fecha de consulta 14 de Mayo de 2013. [En línea]. Disponible en http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2011/common/pdfs/TD-00097-2011_Resolucion-de-fecha-07-03-2011_Art-ii-culo-15-LOPD.pdf

Resoluciones de Tutela de Derechos emitidos por la Agencia Española de Protección de Datos [En línea]. España. Agencia Española de Protección de Datos. Fecha de consulta 30 de Mayo de 2013. [En línea]. Disponible en http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2012/common/pdfs/TD-01846-2011_Resolucion-de-fecha-10-01-2012_Art-ii-culo-16-LOPD.pdf

Resoluciones de Tutela de Derechos emitidos por la Instituto Federal de Acceso a la Información y Protección de Datos [En línea]. México. Fecha de consulta 01 de Junio de 2013. [En línea].Disponible en http://consultas.ifai.org.mx/SesionesspDPTema?tema=14&subtema=2

Resoluciones de Tutela de Derechos emitidos por la Agencia Española de Protección de Datos [En línea]. España. Agencia Española de Protección de Datos. Fecha de consulta 14 de Mayo de 2013. [En línea]. Disponible en http://www.agpd.es/portalwebAGPD/resoluciones/tutela_derechos/tutela_derechos_2013/common/pdfs/TD-02152-2012_Resolucion-de-fecha-20-02-2013_Art-ii-culo-15-LOPD.pdf

MEMORIAS

Memoria de la Agencia Española de Protección de Datos. España. 2011. 112 p.

ARTICULOS

ACED Emilio. Ejercicio y garantía del derecho a la protección de datos personales en el Convenio de Prüm. Revista de derecho constitucional europeo. Nº. 7, 2007. 65-96 p.
FRUTOS Omar. El derecho de cancelación de datos personales en archivos privados en México y España. DERECOM. No 13. Nueva Época. Marzo-Mayo, 2013. [En línea]. Consultada el 15 de Mayo de 2013 en http://www.derecom.com/numeros/pdf/frutos.pdf.

GOMEZ-JUAREZ SIDERA Isidro. Estudio del régimen sancionador de la Ley Orgánica 15/1999 de 13 de diciembre, de protección de datos de carácter personal. Revista española de protección de datos. Thomson Civitas Nº. 4. Enero-Junio de 2008. 133-197 p.

TRONCOSO Antonio. El derecho al olvido en Internet a la luz de la propuesta de Reglamento General de Protección de Datos Personales. Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid., Nº. 59, 2012

ZARATE Sebastián; La problemática entre el derecho al olvido y la libertad de prensa. DERECOM. No 13. Nueva Época. Marzo-Mayo, 2013. [En línea]. Consultada el 16 de Mayo de 2013 en http://www.derecom.com/numeros/pdf/zarate.pdf

GUÍAS

Guía del Responsable de Ficheros. Agencia Española de Protección de Datos. España. 48 p.

Guía de Seguridad de Datos. Agencia Española de Protección de Datos. España. 68 p.

Carta de Servicios. Guía de Seguridad de Datos. Agencia Española de Protección de Datos. España. 32 p.

Guía de Adaptación de la Ley Orgánica de Protección de Datos en las entidades locales. Disponible en línea en http://www.dipsanet.es/cipsa/docs/2008AdaptacionLOPD.pdf. España. Junta de Castilla y León. 2008. 94 p.

Guía de Videovigilancia emitida por la Agencia Española de Protección de Datos disponible en línea en el siguiente sitio electrónico http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf.

PONENCIAS

Primera sesión anual abierta de la Agencia Española de Protección de Datos. 22 de Abril de 2008**.** Fecha de consulta 16 de Mayo de 2013. [En línea]. Disponible en:http://www.agpd.es/portalwebAGPD/jornadas/1_sesion_abierta/common/ponencias_1.pdf

SENTENCIAS

Sentencia del Tribunal de Justicia Europeo de 20 de mayo de 2003 Rechnungshof (asunto C-465/00) Pronunciada en audiencia pública en Luxemburgo Disponible en línea en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62000CJ0465:ES:PDF

ENCUESTAS

Encuesta realizada por la empresa Ipsos Public Affairs para el Instituto Federal del acceso a la información pública y protección de datos en 2012. Preparado para la Secretaría de Protección de datos mediante diversas entrevistas efectivas a hombres y mujeres de 12 años o más y sujetos obligados de diferentes sectores económicos. Consultada el día 27 de Mayo de 2013. Disponible en línea en la siguiente dirección electrónica:
http://inicio.ifai.org.mx/DocumentosIMGSlider/EncuestasNacionalPDP2012.pdf

REVISTAS

Expresión económica. Dossier El Comercio de Datos. Publicación de la Asociación Aragonex. Número 44. Enero 2011 España. 80 p.

ANEXO RELATIVO AL EXPEDIENTE DE PROTECCIÓN DE DERECHOS POR FALTA DE RESPUESTA DEL RESPONSABLE FRENTE A LA SOLICITUD DE ACCESO DE DATOS PERSONALES DESARROLLADO ANTE EL INSTITUTO FEDERAL DE ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS

Con la finalidad de establecer un vinculo teórico-práctico de lo expuesto en la presente investigación se anexa expediente relativo a la solicitud de protección de derechos, específicamente en lo que respecta al derecho de acceso a datos personales del C. Edgar Rodríguez González por la falta de respuesta de la empresa Costco de México S.A. de C.V. . Por lo antes expuesto se inicio procedimiento de tutela efectiva de derechos ante el Instituto Federal de Acceso a la Información y Protección de Datos bajo el expediente PPD.0019/14, del cual se anexan todas las documentales que constituyen las etapas del citado procedimiento, mismas que se relacionan a continuación:

1.- Escrito libre de fecha 10 de Marzo de 2014 en el que se solicita al Instituto Federal de Acceso a la Información y Protección de Datos el procedimiento de protección de derechos interpuesta por el Titular por falta de respuesta del Responsable Costco de México S.A. de C.V..

2.- Acuerdo de fecha 12 de Marzo de 2014en el que se previene al Titular para que en un plazo de cinco días hábiles acreditara su identidad.

3.- Acuerdo de fecha 13 de Marzo en el que se autoriza la vía y dirección de correo electrónico señalada por el titular para recibir notificaciones.

4.-Acuerdo de respuesta del responsable de fecha 9 de Abril de 2014.

5.- Notificación del acuerdo de respuesta del responsable en donde se notifica el acuerdo de respuesta del responsable.

6.- Escrito de fecha 24 de Marzo enviado por el Titular en donde hace las manifestaciones correspondientes en atención a la respuesta del responsable.

7.-Acuerdo de respuesta del responsable de fecha 25 de Abril de 2014 respecto de las manifestaciones hechas por el Titular.

8.- Resolución relativa al Expediente PPD.0019/14 de fecha 07 de Mayo de 2014.