MDTIC

MAESTRÍA EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

“La transferencia de datos personales a través de medios digitales de los servidores públicos obligados pertenecientes a instancias de seguridad nacional. Especial referencia al Instituto Nacional de Migración”

SOLUCIÓN ESTRATÉGICA
Que para obtener el grado de MAESTRO EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Presenta:

Sergio Arturo Martínez Peña

Asesor:

Dra. Evelyn Téllez Carvajal

Ciudad de México, mayo 2023.

CONACYT

INFOTEC POSGRADOS

Autorización de impresión

GOBIERNO DE MÉXICO | CONAHCYT | INFOTEC

AUTORIZACIÓN DE IMPRESIÓN Y NO ADEUDO EN BIBLIOTECA

Maestría en Derecho de las Tecnologías de Información y Comunicación (MDTIC)

Ciudad de México, 26 de mayo de 2023

Unidad de Posgrados
PRESENTE

Por medio de la presente se hace constar que el trabajo de titulación

"La transferencia de datos personales a través de medios digitales de los servidores públicos obligados pertenecientes a instancias de seguridad nacional. Especial referencia al Instituto Nacional de Migración"

Desarrollado por el alumno: **Sergio Arturo Martínez Peña**, y bajo la asesoría de la **Mtra. Evelyn Téllez Carvajal** cumple con el formato de Biblioteca. Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención. Asimismo, se hace constar que no adeuda materiales de la biblioteca de INFOTEC.

No omito mencionar, que se deberá anexar la presente autorización al inicio de la versión impresa del trabajo referido, con el fin de amparar la misma.

Sin más por el momento, aprovecho la ocasión para enviar un cordial saludo.

Mtro. Carlos Josué Lavandeira Portillo
Director Adjunto de Innovación y Conocimiento

CJLP/jah

C.c.p. Felipe Alfonso Delgado Castillo.- Gerente de Capital Humano.- Para su conocimiento
Sergio Arturo Martínez Peña.- Alumno de la Maestría en Derecho de las Tecnologías de Información y Comunicación.- Para su conocimiento.

Agradecimientos

A mi madre, por el apoyo incondicional en todos los proyectos de mi vida.

A mi hermano, por ser ese complemento en mi vida.

A todas las personas que estuvieron cerca y apoyaron este proyecto.

Tabla de contenido

Índice de cuadros

Siglas y abreviaturas

ARCO	Acceso, Rectificación, Cancelación y Oposición
INM	Instituto Nacional de Migración
LGPDPPSO	Ley General de Protección de Datos en Posesión de Sujetos Obligados

Glosario

“A”

ARCO: Derechos Arco para el Acceso, Rectificación, Cancelación y Oposición n de datos personales.

“D”

Dato Personal: Constituye cualquier información concerniente a una persona física identificada o identificable.

Introducción

Con el paso del tiempo, la protección de los datos personales de los individuos ha sido un tema que ha tomado cada vez mayor importancia, pues al tratarse de datos que de manera directa o indirecta puedan identificar a una persona de una manera única, deben ser protegidos por aquellos que por causas legales los obtengan. Éstos no pueden ser mal utilizados vigilando en todo momento la individualidad de la persona.

En la era de la sociedad de la información, los datos personales son cada vez más valiosos, toda vez que constituyen un nuevo campo de explotación en diversos aspectos que van desde el comercial, hasta el criminal.

En México el tema de la protección de los datos personales, surge a partir del 2002 con la publicación en el Diario Oficial de la Federación de la –ya abrogada- Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en la cual por primera vez se refirió a un concepto de dato personal.[1] A partir de aquí, este derecho ha ido avanzando, y cada vez ha sido mayormente regulado ya sea que los datos se encuentren en posesión de particulares o en posesión de entes de gobierno en los tres niveles federal, estatal o municipal.

La regulación normativa en materia de protección de datos personales, se encuentra enfocada principalmente en el entorno a las personas físicas, sin embargo, en el caso de los servidores públicos de la Administración Pública Federal, la legislación ha dejado una laguna al no precisar del todo la manera en que se protegerán sus datos y el uso que se le dan a los mismos. Aún y cuando éstos son personas físicas, el estatus de servidor público, los deja en estado de vulnerabilidad respecto de la transferencia por medios digitales de datos, que, en su caso, se realice de un órgano de gobierno a otro órgano de gobierno aparentemente de manera legal, al no informar de manera detallada el camino que recorren los datos personales de éstos, toda vez que su tratamiento no cumple con los principios de finalidad y tratamiento.

[1] La cual refería en su artículo 3.II que un dato personal constituye “cualquier información concerniente a una persona física identificada o identificable”.

En estos casos, el servidor público queda totalmente vulnerable al no conocer con exactitud el destino de sus datos cuando se realicen transferencias de éstos por medios digitales entre órganos de gobierno, toda vez que son desconocidos para el servidor los lugares en los cuales serán tratados. Con esto queda desprotegido por la normatividad en los casos de que haga mal uso de éstos, ya que para que el servidor público pueda ejercer sus derechos de Acceso, Rectificación, Cancelación y Oposición, en adelante derechos ARCO, debe tener el conocimiento de los lugares en donde han sido tratados dichos datos para poder solicitarlo.

Es por ello, que este trabajo busca identificar que en el tratamiento de los datos personales de los servidores públicos dentro de la Administración Pública Federal, en específico ante el Instituto Nacional de Migración, como instancia de seguridad nacional al ser la solución que se propone en particular, ya que no se cumplen con los principios establecidos en el artículo 16 de la Ley General de Protección de Datos Personales, en Posesión de Sujetos Obligados, en adelante LGPDPPPSO, ya que aún y cuando se trate de servidores públicos, en ningún momento este carácter laboral debe ser óbice para que sus derechos como individuos sean transgredidos.

Los servidores públicos, toda vez que no son informados de manera clara y precisa sobre el tratamiento de los datos personales que son obtenidos por su empleador gubernamental, pueden allegarse de elementos de hecho y de derecho suficientes para poder realizar una acción legal, ante un posible tratamiento ilegal de sus datos al desconocer los lugares en los cuales han sido tratados sus datos personales, y con esto poder ejercer las acciones legales que en cada caso corresponda.

El objetivo general del presente trabajo de investigación es proponer un modelo de solución estratégica para una adecuada transferencia de datos personales de los servidores públicos que laboren en instancias de seguridad nacional, como es el Instituto Nacional de Migración (en adelante INM), que se adapte a la regulación en la materia y con ello dicho personal tenga la facultad de ejercer sus derechos ARCO.

Para efecto de lograr dicho objetivo general, previamente deben alcanzarse los siguientes objetivos específicos:

- Delimitar los alcances y consecuencias jurídicas por la transferencia de datos personales de servidores públicos del Instituto Nacional de Migración entre sujetos obligados
- Identificar que en el tratamiento de los datos personales de los servidores públicos dentro de la Administración Pública Federal, en específico ante el Instituto Nacional de Migración, como instancia de seguridad nacional, no se cumplen con los principios establecidos en el artículo 16 de la LGPDPPSO

En el capítulo 1, se analiza el marco normativo internacional, a efecto de conocer los antecedentes de la protección a la vida privada de las personas, identificando el origen y la evolución de la misma, así como la consecuente evolución de ésta en la normatividad mundial, siendo ésta la protección de los datos personales.

Con la normatividad de la materia de protección de datos personales de sujetos obligados, se busca la protección de los datos personales de las personas ya sea que éstos se encuentren en medio físico o digital, y que su tratamiento sea el adecuado atendiendo a los fines para los que fueren otorgados en cada caso.

En el capítulo 2, se analiza la protección de datos personales en la legislación nacional, identificando en particular la transferencia de datos por medios digitales de los servidores públicos que laboran en instancias de seguridad nacional, en particular el Instituto Nacional de Migración, a efecto de determinar si dicha transferencia vulnera o no los principios del tratamiento de sus datos personales.

Respecto al momento en el que una persona adquiere la calidad de servidor público del Gobierno Federal en una instancia de seguridad nacional, la tutela de protección de datos personales por parte de la normatividad de la materia no es clara, entre las diversas leyes, como son de la de protección de datos personales; de transparencia y acceso a la información y de seguridad nacional. Esto es así, al no establecer cómo el tratamiento de los datos pueda ser realizado por los sujetos obligados, al tratarse de servidores públicos.

En el capítulo 3, se explica el tratamiento de datos personales en el proceso reclutamiento e ingreso en las instancias de seguridad nacional, en particular el INM, así como la transferencia de los datos personales a nivel internacional. También se determinará si en el Instituto Nacional de Migración se cumple con los principios del tratamiento de los datos personales establecidos en la Ley General de Protección de Datos Personales, en Posesión de Sujetos Obligados.

Los servidores públicos del Gobierno Federal, en particular, los de instancias de seguridad nacional previo a ingresar a laborar en una dependencia o entidad, deben presentar diversos documentos que contienen información personal y sensible, poniendo a disposición del empleador datos de carácter patrimonial, y en algunos casos información sensible como datos médicos, religión, preferencias sexuales, los cuales al ser un requisito indispensable para determinar si es un candidato viable para contratar, no puede negarse a la entrega de la misma.

En este tenor, los datos en primera instancia son procesados tanto en medios físicos como medio digitales por el empleador. Sin embargo, los mismos son transferidos a otros sujetos obligados al amparo del artículo 70[2] de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, por tratarse de una instancia de seguridad nacional, sin que el titular de los datos personales conozca el destino específico y el tratamiento de los datos.

De primera mano, se podría justificar dicha transferencia en que los datos personales del individuo son para cumplir con las obligaciones de la instancia de seguridad nacional que los recibe. Sin embargo, el titular de los datos carece de la información sobre la totalidad de los lugares a los cuales serán transferidos por medios electrónicos, ya que sólo se conoce el destino de la institución de seguridad nacional que le corresponda, el Registro Único de Servidores Públicos (RUSP), el

[2] El cual refiere que se podrán realizar transmisiones de datos personales sin el consentimiento del titular y para este caso de estudio nos interesa lo referente de la fracción IX, que a la letra dice:
Artículo 70. El responsable podrá realizar transferencias de datos personales sin necesidad de requerir el consentimiento del titular, en los siguientes supuestos:
… IX. Cuando la transferencia sea necesaria por razones de seguridad nacional.
La actualización de algunas de las excepciones previstas en este artículo, no exime al responsable de cumplir con las obligaciones previstas en el presente Capítulo que resulten aplicables.

registro de alta de plaza ante la Secretaría de Hacienda y Crédito Público, los sistemas de seguridad pública, entre otros.

Con todas estas transferencias el servidor público que labora en instancias de seguridad nacional queda en un estado de indefensión al no conocer quien o quienes tienen sus datos personales, ni el tratamiento que se otorgará a éstos, ya que para poder ejercer los derechos ARCO, debe conocer primero los lugares a los cuales fueron transferidos los datos.

Es por ello, que aún y cuando la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados establece las reglas generales para la transmisión de los datos personales de cualquier persona, no establece el tratamiento que se le darán a los datos cuando se trate de servidores públicos que laboren en instancias de seguridad nacional.

El caso del tratamiento de los datos personales que pertenecen a los servidores públicos que laboren en instancias de seguridad nacional, es un caso *sui géneris*, toda vez que, por un lado, al estar dedicada una persona al servicio público, cumple con las reglas generales como cualquier otro servidor público, sin embargo, adicionalmente a éstos debe de cumplir con diversas obligaciones en varios aspectos, como es el ingreso, la permanencia y su separación (controles de confianza), únicamente establecido para éstas instancias, llevando de manera implícita la transparencia de sus datos, inherentes al cargo que desempeña.

En las diversas legislaciones[3] que se han emitido en materia de transparencia y acceso a la información, así como de protección de datos personales, siempre se ha velado por la protección de los datos ya sea en poder de sujetos obligados, o en su caso, en poder de los particulares.

El tema del tratamiento de los datos personales de los servidores públicos, particularmente en las legislaciones en materia de transparencia y acceso a la información pública, en específico la Ley General de Transparencia y Acceso a la Información Pública (artículo 70) y la Ley Federal de Transparencia y Acceso a la Información Pública (artículos 68 y 69) han sido tratados de una manera particular.

[3] Como la Ley General de Transparencia y Acceso a la Información Pública; Ley Federal de Transparencia y Acceso a la información Pública; Ley General de Protección de Datos en Posesión de Sujetos Obligados; Ley General de Protección de Datos en Posesión de Particulares.

En dichas leyes se han establecido diversas obligaciones generales como específicas, dentro de las cuales se encuentra la publicación de datos personales por parte de los sujetos obligados como parte de las obligaciones de transparencia, así como en su caso, datos relativos a su situación patrimonial.

En este tenor, una persona con el carácter de servidor público en una instancia de seguridad nacional está sujeta a que los datos personales como su nombre, cargo, remuneración económica, sean publicados en los portales de transparencia de los sujetos obligados, para que puedan ser conocidos por cualquier persona de manera precisa y tenga conocimiento de quien ejecuta las actividades del Estado.

En el deber ser, al encontrarse los datos personales en poder de sujetos obligados, los principios y deberes, así como la transmisión se lleva a cabo bajo la titularidad de las legislaciones en materia de datos personales y de transparencia y acceso a la información. Sin embargo, el servidor público de las instancias de seguridad nacional desconoce el camino que recorren sus datos no sólo durante su estancia en éstas, sino que aún después de abandonarlo. Consideramos que no es informado de las diversas instancias en las cuales se encuentran resguardados sus datos, así como el tiempo que permanecerán éstos almacenados en los archivos de los diversos órganos de gobierno, ya sea por sí o por transmisiones entre sujetos obligados.

En este punto las diversas legislaciones en materia de protección de datos como la Ley General de Protección de Datos en Posesión de Sujetos Obligados y la Ley Federal de Protección de Datos en Posesión de Particulares, no han sido precisas en cuanto al tratamiento de los datos de los servidores públicos, ya que se tratan de datos de personas físicas en general, y no se ha establecido que exista una obligación expresa de informar el destino de sus datos, que no solo por el hecho de ser servidor público debe darse por asentado que él conoce su destino o la manera de tratamiento.

Es por ello, que en el transcurso del presente trabajo se analiza la Protección de los Datos Personales entorno a los servidores públicos que laboran dentro de las instancias de seguridad nacional, en específico el Instituto Nacional de Migración

(INM). Describiendo el camino que recorren los datos personales de un servidor público al momento que ingresa a trabajar a dicha instancia de seguridad nacional, estableciendo cuáles son los datos que proporciona al centro de trabajo a su ingreso, la transmisión por medios digitales de éstos entre sujetos obligados y el tratamiento de sus datos personales, lo cual se abordará más adelante.

En el capítulo 4, se explica la transferencia de datos personales a nivel internacional, haciendo especial énfasis en las realizadas por instancias de seguridad nacional de México a instancias de la misma naturaleza de otros países.

En dicho capítulo, se analiza la manera en que se realizan las transferencias de datos personales entre diversos países y la manera en que las mismas son reguladas por la normatividad de la materia.

Lo anterior, sirve como elementos para determinar si las transferencias en las instancias de seguridad nacional de México protegen los datos personales de los servidores públicos.

En el punto 4.4, se explicará un modelo de solución estratégica a efecto de que se pueda dar una solución a la problemática planteada en el presente trabajo de investigación.

En dicho capítulo, se realiza un análisis del proceso que actualmente se encuentra funcionando, y se analiza las probables deficiencias que pudieran observarse en el tratamiento de datos personales, estableciendo en el modelo de solución la manera en cómo se podría dar solución a dicha problemática.

Como hipótesis tenemos que la transferencia de datos personales de los servidores públicos a través de medios digitales que laboran en instancias de seguridad nacional, en específico el INM entre sujetos obligados de la Administración Pública Federal, se realiza sin solicitar el consentimiento expreso de éstos, o en su caso, con el aviso de que los datos serán transferidos a otros entes, siendo entonces que se tiene desconocimiento de estas transferencias.

Dicha situación no puede ser omitida con la justificación de que se trata de un tema de seguridad nacional, toda vez que el hecho de que sea catalogado con dicha salvaguarda, no implica que no se informe a los servidores públicos el destino final y el tratamiento de sus datos personales.

En este tenor, tenemos que, al realizarse la transferencia de datos personales de los servidores públicos entre sujetos obligados, puede llegar a existir una omisión al derecho de protección de datos personales al no informar al titular de los datos personales su destino y tratamiento de los mismos, así como el consentimiento expreso, en los casos que se requiera, mismo que no es requisito necesario en los casos que establece el artículo 22 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados,[4] sin embargo, en la fracción I, se establece que para dicha transferencia se deberán respetar los principios de la ley, siendo que al no respetarse el principio de finalidad, como adelante veremos, no se cumplen con dichos principios, esto es que en los casos de excepción debiera dar aviso del lugar al cual serán transferidos los datos.

En este caso, estaríamos ante una violación al principio de finalidad, toda vez que, al realizarse la transferencia de datos personales por medios digitales de los servidores públicos entre sujetos obligados, sin la existencia del consentimiento expreso de los titulares, o en su caso, al no informar el lugar al cual serán transferidos, y no precisar la finalidad del tratamiento y mucho menos el tiempo de éste, no se actualiza el supuesto del artículo 18 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados al no justificarse las finalidades concretas y explícitas relacionadas con las atribuciones de una instancia de

[4] Artículo 22. El responsable no estará obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales en los siguientes casos:

I. Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley, en ningún caso, podrán contravenirla;
II. Cuando las transferencias que se realicen entre responsables sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;
III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
IV. Para el reconocimiento o defensa de derechos del titular ante autoridad competente;
V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;
VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
VII. Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria;
VIII. Cuando los datos personales figuren en fuentes de acceso público;
IX. Cuando los datos personales se sometan a un procedimiento previo de disociación, o
X. Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.

seguridad nacional, como es el caso del INM, como se abordará en el desarrollo del presente trabajo.

Lo anterior, pareciera contradictorio con lo establecido en el mencionado artículo 22 de la LGPDPPSO, sin embargo, no es así, toda vez que se establecen las causas en las cuales no existe obligación de recabar el consentimiento expreso, más no el hecho de no informar al titular de los datos el tratamiento y el destino que se le darán a sus datos.

- Cuando la transmisión de datos personales entre sujetos obligados por medios digitales se realice bajo la justificación de cuestiones de seguridad nacional o por alguna ley que así lo establezca.

Este supuesto sería el caso de excepción, cuando por causas de seguridad nacional sea necesaria la recolección de datos personales en posesión de otros sujetos obligados y se solicite su transferencia por medios digitales sin el consentimiento del titular de los datos, sin embargo, no se exime que sea notificado del tratamiento que se les dará, ni del periodo de conservación.

- Cuando los datos personales de los servidores públicos sean publicados o entregados en cumplimiento con obligaciones de transparencia.

Esto es, que ya sea a través de las obligaciones de transparencia de los sujetos obligados o a través de una solicitud de acceso a la información sean publicitados los datos personales del servidor público titular de los datos.

Puede presentarse alguna variable como la siguiente:

- Cuando una ley así lo disponga la transferencia de datos personales de los servidores públicos.

Esto es, cuando derivado de alguna disposición de alguna otra ley o convenio concreto distintos a los de acceso a la información y protección de datos personales, sea establecida la transferencia de los datos personales de los servidores públicos.

Capítulo 1.

Epítome de la Protección de Datos Personales

Capítulo 1. Epítome de la Protección de Datos Personales

En el presente capítulo analizaremos la evolución de la protección de datos personales a través de los años, identificando como fue estableciéndose de manera más clara dicha protección en la normatividad a nivel mundial.

Identificaremos el origen de la protección de los datos personales, así como son protegidos a nivel internacional y a nivel nacional, siendo el caso particular de México, y en el caso particular, el tema de protección de datos personales de los servidores públicos que laboran en instancias de seguridad nacional como es el Instituto Nacional de Migración.

Asimismo, veremos la manera en cómo en México se ha ido estableciendo de manera más precisa la normatividad en materia de datos personales y la protección de éstos.

1.1 Breve génesis de la Protección de Datos Personales a nivel internacional

La protección de datos personales como la conocemos hoy en día tiene como base la protección a la vida privada de las personas, la cual fue reconocida en diversas normatividades a nivel internacional como son la Declaración Universal de los Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos.

De la misma manera el Parlamento de Europa y el Consejo, a través de diversas normativas realizan el reconocimiento a la protección de la vida privada de las personas, así como a los datos personales y el tratamiento de los mismos.

Dentro de lo más relevante de dichas disposiciones es la obligación de los Estados de garantizar la protección de los datos personales a través de sus instituciones, como a continuación lo abordaremos.

1.1.1 Declaración Universal de los Derechos Humanos

La Declaración Universal de los Derechos Humanos emitida en 1948 en el seno de la Organización de las Naciones Unidas, resalta la protección de la vida privada de la persona. Para el caso que nos ocupa, el artículo 12 refiere: “Nadie podrá ser objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su

correspondencia, ni de ataques a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".[5]

En este artículo podemos observar como la Declaración realiza un reconocimiento expreso del derecho de protección de la vida privada de la persona, señalando que como vida privada está integrada por varios elementos (familia, domicilio, correspondencia, honra, reputación). Esta disposición es el origen al reconocimiento de la protección a la vida privada de toda persona y que ésta no sea susceptible de intromisiones ya sea por parte del gobierno o de otras personas.

Es de señalar, que aún y cuando se trata de un documento no vinculante, sirve de referencia para determinar que existe un reconocimiento a la vida privada de las personas, la cual no puede ser vulnerada de manera arbitraria.

Lo anterior, se puede entender ya que, al reconocerse una protección de vida privada, dentro de estos elementos que la integran, es decir la parte íntima de las personas se encuentran los aspectos de cada persona como su religión, su salud, sus costumbres, así como los datos del individuo, los cuales deben ser protegidos para que éstos no sean vulnerados, ya que de manera aislada quizás no representen ningún problema, pero al asociarse puede dar lugar a identificar a una persona, como lo menciona el autor Fulgencio Madrid Conesa "existen datos que *a priori* son irrelevantes desde el punto de vista del derecho a la intimidad, pero que unidos unos con otros, pueden servir para configurar una idea prácticamente completa de cualquier individuo, al igual que ocurre con las pequeñas piedras que forman un mosaico, que en sí no dicen nada, pero que unidas pueden formar conjuntos plenos de significado".[6]

---

5 Naciones Unidas. *Declaración Universal de Derechos Humanos.* http://www.un.org/es/universal-declaration-human-rights/ (Consultada el 25 de enero de 2018).

6 Madrid Conesa, Fulgencio, *Derecho a la intimidad, informática y Estado de derecho*, Valencia, Universidad de Valencia, 1984, p. 45.

1.1.2 Pacto Internacional de Derechos Civiles y Políticos

En el año 1966 se celebró el Pacto Internacional de Derechos Civiles y Políticos, en el cual en su artículo 17, establece lo siguiente:

> "1. Nadie será objeto de injerencias arbitrarias o legales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.
>
> 2. Toda persona tiene Derecho a la protección de la ley contra esas injerencias o ataques."[7]

Es evidente que el texto del Pacto Internacional es muy similar a lo establecido en la Declaración Universal de los Derechos Humanos (DUDH), lo cual no es casuístico, ya que se trata de documentos con el interés de proteger los derechos humanos, en el caso que nos interesa, la vida privada de los individuos. Sin embargo, este Pacto a diferencia de la Declaración Universal de los Derechos Humanos, si es de carácter vinculante para aquellos Estados que lo suscriban, por lo cual, en este caso, tenemos que este es el principio de la regulación de la protección de la vida privada, de manera formal. El autor Humberto Quira Lavié define la intimidad de la siguiente manera; "el respeto a la personalidad humana, del aislamiento del hombre, de lo íntimo de cada uno, de la vida privada, de la persona física, innata, inherente y necesaria para desarrollar su vida sin entorpecimientos, perturbaciones y publicidades indeseadas".[8]

Para el caso que nos ocupa, es de suma importancia este Pacto, toda vez que al establecer en el mismo la protección en contra de injerencias arbitrarias o legales en su vida privada, se le otorga el derecho a cualquier persona de protección a ésta, incluyendo aquellas injerencias que se realicen con apego a alguna ley o mandato legal, ya que el precisar que "toda persona tiene derecho a la protección

---

[7] Naciones Unidas. Pacto Internacional de Derechos Civiles y Políticos. https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights (Consultada el 25 de enero de 2018)

[8] Quiroga Lavié, Humberto, *Derecho a la intimidad y objeción de conciencia*, Bogotá: Universidad Externado de Colombia, 1995), p. 10.

de la ley contra esas injerencias o ataques", es la base de la protección de la vida privada.

La importancia del mencionado Pacto es el haber reconocido la protección de la vida privada de la persona, con todos los elementos que la integran, en este tenor, el autor Luis Meján conceptualiza el derecho a la intimidad diciendo que "...es un Derecho Fundamental que asiste a los sujetos de derecho consistente en la facultad de mantener en reserva sobre diversas situaciones relacionadas con la vida privada, que debe ser reconocido y regulado por el sistema jurídico y que es oponible a todos los demás salvo en los casos en que puede ser develado por existir un derecho superior de terceros o para el bienestar común". [9]

Para el caso particular que nos ocupa, al momento de ingresar a laborar en una instancia de seguridad nacional como lo es el Instituto Nacional de Migración, nos encontramos ante una injerencia en la vida privada de las personas, toda vez que como parte de los requisitos de ingreso se solicitan datos respecto de la vida privada de las personas, como es religión, salud, costumbres, aficiones, salud, economía, preferencias sexuales, datos personales. Toda esta información queda resguardada en el centro laboral tanto en la duración del encargo, así como después de que se separó del cargo.

1.2. Convenio 108 Para la Protección de las Personas con respecto al tratamiento automatizado de los datos de carácter personal

En 1981 el Consejo de Europa aprueba el "Convenio 108 para la Protección de las Personas con respecto al tratamiento automatizado de los datos de carácter personal", el cual tiene como objeto garantizar a todas las personas físicas, el respeto de los derechos y libertades fundamentales, siendo especialmente cuidado el derecho a la vida privada del individuo en el tratamiento automatizado de los datos personales de todos aquellos ficheros automatizados que contengan información

[9] Mejan, Luis Manuel C., *El Derecho a la Intimidad y la Informática*, México, Porrúa, 1994, p. 69.

personal tanto en el sector público como en el privado. Así como para tener una coincidencia de la protección a la vida privada de las personas y que la circulación de los datos de éstas sea de una manera segura tanto entre los Estados miembros de este Convenio, así como de aquellos que no estén adheridos a éstos (artículo 1, 3 y 12).[10]

Este texto es muy relevante, toda vez que por primera ocasión se establece en un documento internacional la protección de los datos personales de los individuos. Asimismo, se establece que los Estados adheridos al Convenio pueden intercambiar datos (artículo 12), vigilando en todo momento la integridad de éstos, también establece que no podrán ser compartidos con aquellos que no sean partícipes del instrumento legal, a efecto de evitar su mal uso.

En este Convenio se establece que los datos deberán ser obtenidos de manera leal y legítimamente, los cuales serán conservados en ficheros, indicando que la forma que se permitirá la identificación de las personas, señalando que sólo se podrán guardar los datos durante un período de tiempo que no exceda del

10 Artículo 1. Objeto y fin
El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona («protección de datos»).
Artículo 3. Campos de aplicación
1. Partes se comprometen a aplicar el presente Convenio a los ficheros y a los tratamientos automatizados de datos de carácter personal en los sectores público y privado.
2. Cualquier Estado podrá en el momento de la firma o al depositar su instrumento de ratificación, aceptación, aprobación o adhesión, o en cualquier otro momento ulterior- hacer saber mediante declaración dirigida al Secretario general del Consejo de Europa:
a) Que no aplicará el presente Convenio a determinadas categorías de ficheros automáticos de datos de carácter personal, una lista de las cuales quedará depositada. No deberá sin embargo incluir en esa lista categorías de ficheros automatizados sometidas, con arreglo a su derecho interno, a disposiciones de protección de datos. Deberá, por tanto, modificar dicha lista mediante una nueva declaración cuando estén sometidas a su régimen de protección de datos categorías suplementarias de ficheros automatizados de datos de carácter personal;
b) que aplicará el presente Convenio, asimismo, a informaciones relativas a agrupaciones, asociaciones, fundaciones, sociedades, compañías o cualquier otro organismo compuesto directa o indirectamente de personas físicas, tengan o no personalidad jurídica;
c) que aplicará el presente Convenio, asimismo, a los ficheros de datos de carácter personal que no sean objeto de tratamientos automatizados.
3. Cualquier Estado que haya ampliado el campo de aplicación del presente Convenio mediante una de las declaraciones a que se refieren los apartados 2, b) o c), que anteceden podrá, en dicha declaración, indicar que las ampliaciones solamente se aplicarán a determinadas categorías de ficheros de carácter personal cuya lista quedará depositada.

necesario para las finalidades para las cuales se hayan registrado, situación que es sumamente importante ya que no puede ser infinito el tiempo en que se resguarden los datos personales; esto es, será acorde el tiempo de guarda con el fin a utilizar (artículo 5).[11]

Otro punto importante, es que se establece que los datos personales que pongan de manifiesto el origen racial o étnico, el criterio político, las creencias religiosas, los datos personales de salud y/o vida sexual, no pueden ser tratados de manera automática, con la salvedad que el derecho interno establezca garantías para los titulares de los datos. Esto es muy relevante en el tema de tratamiento de datos personales sensibles ya que dichos datos deberán ser cuidadosamente resguardados y manejados de una manera separada e independiente de los datos personales recopilados, lo cual se traduce en salvaguardar los aspectos más íntimos de las personas (artículo 6).[12]

Además este Convenio señala que las personas deben conocer la existencia del fichero automatizado que contiene sus datos personales, las finalidades del uso de los datos, así́ como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero, señalando que cada determinado tiempo (intervalos razonables y sin demora o gastos excesivos) la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que

[11] Artículo 5. Calidad de los datos
Los datos de carácter personal que sean objeto de un tratamiento automatizado:
a) Se obtendrán y trataran leal y legítimamente;
b) se registraran para finalidades determinadas y legítimas, y no se utilizaran de una forma incompatible con dichas finalidades;
c) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado;
d) serán exactos y si fuera necesario puestos al día;
e) se conservarán bajo una forma que permita la identificación de las personas concernidas durante un periodo de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado".

[12] Artículo 6. Categorías particulares de datos
Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así́ como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá́ en el caso de datos de carácter personal referentes a condenas penales."

conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible (artículo 8).[13]

De lo anterior, se puede observar que cualquier persona de la cual sean recopilados sus datos personales, tiene el derecho de conocer en todo momento cómo se recopilan, el uso, el estatus real, los fines y la autoridad que resguarda sus datos personales, lo cual es la autodeterminación la cual la podemos entender como "aquella necesidad de que los ciudadanos controlen la información que les concierne, ya no como un mero derecho de defensa frente a las intromisiones de otros, sino ahora, y frente a los riesgos tecnológicos, como un derecho activo de control sobre el flujo de informaciones que circulan sobre nosotros".[14]

El 12 de junio de 2018 México ratificó dicho Convenio, por lo cual ya forma parte del mismo.

De lo anterior, tenemos que México al haber ratificado dicho Convenio tiene la obligación de informar a todas las personas, en particular del caso que nos ocupa a los servidores públicos que trabajen en el Instituto Nacional de Migración, los lugares en los cuales se encuentran almacenados sus datos personales, así como las instituciones que tengan acceso a ellos, es decir, el INM tiene la obligación de informar a cada servidor público, a los lugares a los cuales han sido transferidos los datos personales.

---

[13] Artículo 8. Garantías complementarias para la persona concernida
Cualquier persona deberá poder:
a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero;
b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible;
c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio;
d) disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de ratificación o de borrado, a que se refieren los párrafos b y c del presente artículo.

[14] Winfried Hassemer, *El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales,* Buenos Aires: Editores del Puerto, 1997, p. 124.

Por otra parte, también se debe establecer el tiempo que estarán en dichos ficheros y una vez cumplidos con sus fines, deberá notificarse que los mismos serán destruidos, situación que no acontece así, ya que el servidor público no es informado de dicha situación, y por lo cual no se tiene certeza de los lugares en los cuales se encuentran almacenados dichos datos, situación que vulnera sus derechos.

1.3 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.

El 24 de octubre de 1995, el Parlamento Europeo y el Consejo de Europa publicaron la Directiva 95/46/CE relativa a la protección de datos personales de las personas físicas y a la libre circulación de éstos. La importancia de esta Directiva radica que se incluyó un nuevo término que es el derecho a la intimidad tanto de la persona como a la intimidad informática, de manera general se explica los alcances de ésta.

Esta Directiva tenía como objeto proteger los derechos y las libertades de las personas en lo que respecta al tratamiento de sus datos personales, cuidando que el tratamiento sea lícito en apego los principios de la calidad de los datos.

Dicha Directiva era aplicable a los datos que son tratados por medios automatizados o en papel. Estableciendo como excepción de aplicación a ésta cuando sea realizado por una persona física en actividades particulares o domésticas, así como cuando se trate de la seguridad pública, la defensa o la seguridad del Estado (artículo 3).

En este instrumento se puede observar que se estableció que para que el tratamiento de los datos pueda ser lícito, debe vigilar que se cumplan con los siguientes principios (artículo 7):

- Exista consentimiento de la persona;

- El tratamiento sea necesario para el cumplimiento de un contrato en el que el titular de los datos sea parte o para el cumplimiento de una obligación legal del responsable del tratamiento;
- Para proteger los intereses vitales de la persona titular de los datos;
- Para el cumplimiento de un encargo de interés público o relativo al ejercicio del poder público del responsable o un tercero;
- Para los fines legales del responsable del tratamiento o de un tercero.

La Directiva establece que los datos personales serán tratados de manera leal y lícita, con fines determinados, explícitos y legítimos, siendo éstos adecuados, pertinentes, no excesivos, exactos, actualizados, y para un periodo determinado (artículo 6).

Por otra parte, establece que no se podrán tratar datos personales como origen racial, religión, opiniones políticas, pertenencia a sindicatos, datos relativos a salud o sexualidad, estableciendo como excepción de cuando si se podrán tratar los datos cuando sea necesario para salvaguardar el interés vital del titular de los datos (artículo 8).

En el mismo tenor, se establece que el titular de los datos puede ejercer el derecho a obtener información, así como el derecho de acceso y el de oponerse al tratamiento de los datos. Se indica como excepción para los derechos de los titulares cuando se trate de salvaguardar la seguridad del Estado, la defensa, a la seguridad pública, entre otros (artículos 12 y 14).

Por lo que respecta a la transferencia de datos personales, se establece la posibilidad de transferirlos a un tercer país, en los siguientes términos:

> *"Se autorizará la **transferencia de datos personales** de un Estado miembro **a un tercer país** que garantice un nivel de protección adecuado; por el contrario, si bien no se autoriza la transferencia cuando no se garantice un nivel adecuado de protección, esta norma tiene varias excepciones que se enumeran en la Directiva; p. ej. cuando el propio interesado consienta la transferencia, en el caso de la celebración de un contrato, cuando sea*

necesario por motivos de interés público y también si el Estado miembro ha autorizado normas empresariales vinculantes o cláusulas contractuales."[15]

Es de resaltar, que la Directiva arriba citada retoma el proceso de protección de los datos personales cuando sean tratados a través de sistemas automatizados del Convenio 108, esto con el objeto de que los datos de las personas no sean transmitidos de manera indiscriminada y no se haga un mal uso de éstos.

En este caso del documento en comento, es de resaltar que se establece que no será aplicable la misma cuando se refiere de datos tratados por medios automatizados realizados por una persona física en el ejercicio de sus actividades, o cuando sean actividades para salvaguardar el interés público, lo cual, expone las excepciones para su aplicación. Esto es que cuando los datos personales se encuentren en una base sistematizada si son recabados por personas físicas no será aplicable, siendo que si se trata de una persona moral si será aplicable, sin embargo, el hecho de la naturaleza de la persona ya sea física o moral no es óbice, para que en ambos casos puedan ser mal utilizados los datos personales, ya que no se trata de quien los recopile, sino el uso final de éstos (artículo 26).

Esta Directiva es citada, aún y cuando la misma ya no se encuentra vigente, toda vez que sirve de referencia para identificar cómo el Parlamento Europeo, en su búsqueda de proteger los datos personales de las personas, en el manejo de la información cuando se encontraba en ficheros físicos, pero más aún cuando esta información se encontraba en ficheros electrónicos; dictó esta norma para regular el manejo y transmisión de los datos personales entre países miembros del Consejo, así como con países externos, estableciendo los requisitos para el tratamiento de los datos.

1.4 Carta de los Derechos Fundamentales de la Unión Europea

En diciembre del año 2000, el Parlamento Europeo, el Consejo de Europa y la Comisión Europea, proclamaron la Carta de los Derechos Fundamentales de la

[15] EUR-Les Access to European Union law, Protección de los datos personales. Directiva 95/46/CE, en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3Al14012 (consultada el 27 de julio de 2018).

Unión Europea. Este documento es de suma importancia, toda vez que con éste se busca que los países miembros de la Unión Europea puedan convivir en armonía y bajo el respeto de los derechos fundamentales para las personas europeas (artículos 3, 7 y 8).

En sus artículos 3, 7 y 8, se establece lo siguiente:

Artículo 3

Derecho a la integridad de la persona

1. Toda persona tiene derecho a su integridad física y psíquica.

2. En el marco de la medicina y la biología se respetarán en particular:

- el consentimiento libre e informado de la persona de que se trate, de acuerdo con las modalidades establecidas en la ley,

- la prohibición de las prácticas eugenésicas, y en particular las que tienen por finalidad la selección de las personas,

- la prohibición de que el cuerpo humano o partes del mismo en cuanto tales se conviertan en objeto de lucro,

- la prohibición de la clonación reproductora de seres humanos.

Artículo 7

Respeto de la vida privada y familiar

Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.

Articulo 8

Protección de datos de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legitimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3. El respeto de estas normas quedará sujeto al control de una autoridad independiente. [16]

[16] Diario Oficial de las Comunidades Europeas, en http://www.europarl.europa.eu/charter/pdf/text_es.pdf (consultada el 20 de septiembre de 2018).

Como se puede observar, el artículo 3 establece “dos puntos importantes en la protección de datos personales, siendo que el primer punto reconoce el derecho independiente a la privacidad.”

Asimismo, en el artículo 7 se “reconoce el derecho de protección al respeto de su vida privada y familiar, siendo que en artículo 8 se establece que toda persona tiene derecho a la protección de los datos personales; esto es, ya no sólo se trata del derecho a la privacidad de la persona, sino que ahonda más y abarca a los datos personales de las personas.”

En este tenor, algo sumamente importante, es establecer que la autoridad independiente es la encargada de vigilar los datos personales, lo cual es lo más transparente en este tipo de casos.

Por otra parte, establece temas que son la naturaleza de los derechos fundamentales de la protección de datos personales, como el fin de los datos recolectados, el tratamiento de los mismos, el acceso de los datos por parte de los titulares, así como la rectificación de los datos.

1.5 Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

En diciembre del año 2000, se publicó el Reglamento No. 45/2001, relativo a la Protección de las Personas en el Tratamiento de Datos Personales, en este caso haciendo la precisión de que se trata del tratamiento realizado por instituciones y órganos comunitarios.

En virtud de que este Reglamento es aplicable a las “instituciones y organismos comunitarios” respecto a la intimidad y protección de datos personales, sirve como una pauta para el trabajo que se desarrolla como a continuación expondremos.

Es de resaltar que con este Reglamento se busca garantizar el cumplimiento de la normatividad en materia de protección a los datos personales entre los Estados miembros de la Comunidad Europea. En ese sentido determina claramente los principios de los datos personales como la licitud y los fines (artículos 1, 4, 5, 6, 7, 8 y 9).

En el artículo 1, se establece que "las instituciones y los organismos creados por los tratados de las Comunidades Europeas, conforme a dicho reglamento garantizarán la protección de datos, así como el derecho a la intimidad, no limitando ni prohibiendo la libre circulación de los mismos entre ellos o los miembros adoptados por la Directiva 95/46/CE. La autoridad encargada de verificar lo anterior, será el Supervisor Europeo de Protección de Datos."[17]

El mencionado Reglamento establece la calidad de los datos personales, siendo que los mismos deben ser tratados de manera leal y lícita; recogidos con fines determinados, explícitos y legítimos; adecuados, pertinentes y no excesivos; exactos; no conservados por un periodo mayor para los fines originales.[18]

---

[17] Artículo 1 **Objeto del Reglamento**
1. Las instituciones y los organismos creados por los Tratados constitutivos de las Comunidades Europeas o en virtud de dichos Tratados, en lo sucesivo denominados «instituciones y organismos comunitarios», garantizarán, de conformidad con el presente Reglamento, la protección de los derechos y las libertades fundamentales de las personas físicas, y en particular su derecho a la intimidad, en lo que respecta al tratamiento de los datos personales, y no limitarán ni prohibirán la libre circulación de datos personales entre ellos o entre ellos y destinatarios sujetos al Derecho nacional de los Estados miembros adoptado en aplicación de la Directiva 95/46/CE.
2. La autoridad de control independiente establecida por el presente Reglamento, en lo sucesivo denominada Supervisor Europeo de Protección de Datos», supervisará la aplicación de las disposiciones del presente Reglamento a todas las operaciones de tratamiento realizadas por las instituciones y organismos comunitarios.

[18] Artículo 4
Calidad de los datos
1. Los datos personales deberán ser:
a) tratados de manera leal y lícita;
b) recogidos con fines determinados, explícitos y legítimos, y no ser tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando el responsable del tratamiento establezca las garantías oportunas, en particular para asegurar que los datos no serán tratados con otros fines y que no se utilizarán en favor de medidas o decisiones que afecten a personas concretas;
c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente;
d) exactos y, si fuera necesario, actualizados; se tomarán todas las medidas razonables para la supresión o rectificación de los datos inexactos o incompletos en relación con los fines para los que fueron recogidos o para los que son tratados posteriormente;

Asimismo, establece que el tratamiento de los datos personales solo puede efectuarse si es necesario para un tema de interés público; así como si es necesario para el cumplimiento de una obligación jurídica; o en caso de la celebración de un contrato en el que el titular de los mismos sea parte; el interesado haya dado su consentimiento inequívocamente; o para proteger al titular.[19] En caso de que existieran cambios a los fines para los que fueron recolectados los datos, esto siempre y cuando esté establecido en las normas de la institución o en caso de los datos utilizados para la seguridad o control, sólo se podrán usar para la prevención, investigación de infracciones penales.[20]

Por otra parte, se establece que la transmisión de datos entre las instituciones y organismos comunitarios, sólo se dará si son necesarios dentro del ámbito de

---

e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para la consecución de los fines para los que fueron recogidos o para los que se traten posteriormente. La institución o el organismo comunitario establecerá para los datos personales que deban ser archivados por un período más largo del mencionado para fines históricos, estadísticos o científicos, que dichos datos se archiven bien únicamente en forma anónima, o, cuando ello no sea posible, sólo con la identidad codificada del interesado. En cualquier caso, deberá imposibilitarse el uso de los datos salvo para fines históricos, estadísticos o científicos.
2. Incumbirá al responsable del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1.

[19] *Artículo 5*
Licitud del tratamiento de datos
El tratamiento de datos personales sólo podrá efectuarse si:
a) es necesario para el cumplimiento de una misión de interés público en virtud de los Tratados constitutivos de las Comunidades Europeas o de otros actos legislativos adoptados sobre la base de los mismos o es inherente al ejercicio legítimo del poder público conferido a la institución o al organismo comunitario o a un tercero a quien se comuniquen los datos, o
b) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o
c) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o
d) el interesado ha dado su consentimiento de forma inequívoca, o
e) es necesario para proteger los intereses esenciales del interesado.
[20] *Artículo 6*
Cambio de fines
Sin perjuicio de lo dispuesto en los artículos 4, 5 y 10:
1) Los datos personales sólo podrán tratarse con fines distintos de los que motivaron su recogida cuando este cambio de fin esté permitido expresamente por normas internas de la institución o del organismo comunitario.

2) Los datos personales recogidos exclusivamente para garantizar la seguridad o el control de los sistemas o las operaciones de tratamiento no se utilizarán con ningún otro fin, salvo los de la prevención, la investigación, la detección y la represión de infracciones penales graves.

competencia del destinatario, siendo la responsabilidad de ambas partes la misma, estableciendo reglas para ésta.[21]

También se establece la transmisión de datos personales para organismos distintos a las instituciones comunitarias que son sujetos a la Directiva 95/46/CE, teniendo como requisitos que el destinatario deberá demostrar que son para cumplir el interés público y que no exista perjuicio en los intereses legítimos del interesado.[22]

Por otra parte, se establece que para que puedan transmitirse los datos personales a instituciones u organismos no comunitarios y no sujetos a la Directiva 95/46/CE, debe garantizarse protección suficiente para éstos en el país de destino y sólo para el ejercicio de las tareas del destinatario, tomándose en cuenta la naturaleza de los datos, la finalidad y la duración de las operaciones de tratamiento, la normatividad del país u organización destino.

En caso de que el titular de los datos personales, haya dado su consentimiento de forma inequívoca se podrá realizar la transmisión, así como cuando la misma sea necesaria para la celebración o la conclusión de un contrato entre el titular y el responsable del tratamiento; así como razones de interés público

---

[21] *Artículo 7*

Transmisión de datos personales entre las instituciones o los organismos comunitarios o en el seno de dichas instituciones y organismos

Sin perjuicio de lo dispuesto en los artículos 4, 5, 6 y 10:

1) Los datos personales sólo se transmitirán a otras instituciones y organismos comunitarios o en el seno de dichas instituciones y organismos si son necesarios para el ejercicio legítimo de las tareas que pertenecen al ámbito de competencia del destinatario.

2) Cuando los datos se transmitan a petición del destinatario, la responsabilidad relativa a la legitimidad de la transmisión incumbirá tanto al responsable del tratamiento como al destinatario. El responsable del tratamiento estará obligado a verificar la competencia del destinatario y a efectuar una evaluación provisional de la necesidad de la transmisión de dichos datos. En caso de abrigar dudas sobre tal necesidad, el responsable del tratamiento pedirá al destinatario que aporte información complementaria. El destinatario garantizará la posibilidad de verificar subsiguientemente la necesidad de la transmisión de los datos.

3) El destinatario tratará los datos personales únicamente para los fines que hayan motivado su transmisión.

[22] *Artículo 8*

Transmisión de datos personales a destinatarios, distintos de las instituciones y los organismos comunitarios, sujetos a la Directiva 95/46/CE

Sin perjuicio de lo dispuesto en los artículos 4, 5, 6 y 10, los datos personales sólo se transmitirán a destinatarios sujetos al Derecho nacional adoptado para la aplicación de la Directiva 95/46/CE, cuando:

a) el destinatario demuestre que los datos son necesarios para el cumplimiento de una misión de interés público o son inherentes al ejercicio del poder público, o

b) el destinatario demuestre la necesidad de que se le transmitan los datos y no existan motivos para suponer que ello pudiera perjudicar los intereses legítimos del interesado.

importante, o en caso de algún ejercicio o defensa en algún procedimiento judicial.[23]

[23] *Artículo 9*

Transmisión de datos personales a destinatarios distintos de las instituciones y los organismos comunitarios y no sujetos a la Directiva 95/46/CE

1. Los datos personales sólo se podrán transmitir a destinatarios distintos de las instituciones y los organismos comunitarios y no sujetos al Derecho nacional adoptado en aplicación de la Directiva 95/46/CE cuando se garantice un nivel de protección suficiente en el país del destinatario o en la organización internacional destinataria, y los datos se transmitan exclusivamente para permitir el ejercicio de las tareas que son competencia del responsable del tratamiento.

2. La suficiencia del nivel de protección ofrecido por el tercer país o la organización internacional de que se trate se determinará a la luz de todas las circunstancias que rodean la operación de transmisión de datos o el conjunto de operaciones de transmisión de datos. Se tendrá particularmente en cuenta la naturaleza de los datos, la finalidad y la duración de las operaciones de tratamiento propuestas, el tercer país o la organización internacional de destino final, los preceptos legales generales y sectoriales vigentes en el tercer país o aplicables a la organización internacional de que se trate, así como las normas profesionales y las medidas de seguridad observadas en ese país u organización internacional.

3. Las instituciones y los organismos comunitarios informarán a la Comisión y al Supervisor Europeo de Protección de Datos de los casos en los que a su entender el tercer país o la organización internacional de que se trate no garanticen un nivel de protección suficiente de acuerdo con el apartado 2.

La Comisión informará a los Estados miembros de los casos contemplados en el apartado 3.

Las instituciones y los organismos comunitarios tomarán las medidas oportunas para cumplir las decisiones adoptadas por la Comisión en las que se haga constar, en aplicación de los apartados 4 y 6 del artículo 25 de la Directiva 95/46/CE, que un tercer país o una organización internacional garantizan o no garantizan un nivel de protección suficiente.

6. No obstante lo dispuesto en los apartados 1 y 2, la institución o el organismo comunitario podrá efectuar una transmisión de datos personales si:

a) el interesado ha dado su consentimiento de forma inequívoca a la transmisión propuesta; o

b) la transmisión es necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la aplicación de medidas precontractuales a petición del interesado; o

c) la transmisión es necesaria para la conclusión o ejecución de un contrato concluido en interés del interesado entre el responsable del tratamiento y un tercero; o

d) la transmisión es necesaria o requerida legalmente por razones importantes de interés público o para el reconocimiento, el ejercicio o la defensa de un derecho en un procedimiento judicial; o

e) la transmisión es necesaria para proteger los intereses esenciales del interesado; o

f) la transmisión se realiza desde un registro que, con arreglo al Derecho comunitario, tenga por objeto proporcionar información al público y que esté disponible para consulta del público en general o de cualquier persona que pueda demostrar un interés legítimo, en la medida en que en ese caso particular se cumplan las condiciones de consulta fijadas en la legislación comunitaria.

7. Sin perjuicio de lo dispuesto en el apartado 6, el Supervisor Europeo de Protección de Datos podrá autorizar una transferencia o conjunto de transferencias de datos personales a un tercer país o a una organización internacional que no garanticen un nivel de protección adecuado en el sentido de los apartados 1 y 2 cuando el responsable del tratamiento ofrezca garantías suficientes con respecto a la protección de la vida privada y los derechos y las libertades fundamentales de las personas, así como por lo que respecta al ejercicio de los derechos correspondientes; estas garantías pueden, en particular, resultar de cláusulas contractuales pertinentes.

8. Las instituciones y los organismos comunitarios informarán al Supervisor Europeo de Protección de Datos de las categorías de casos en que hayan aplicado los apartados 6 y 7.

Menciona que su aplicación es para los ficheros semi y automatizados en los cuales se encuentren los diversos datos personales. Así también establece como es aplicable respecto de la confidencialidad de las comunicaciones (artículo 3).

En el artículo 20.1 inciso d), se establece como causal de excepción del tratamiento leal y licito, así como de la información que se deba dar al interesado respecto de los datos recolectados o en su caso cuando no han sido recabados por el interesado y el derecho de acceso, cuando se trate de medida necesaria para la seguridad nacional, mismo que a continuación se reproduce:

"Artículo 20

Excepciones y limitaciones

1. Las instituciones y los organismos comunitarios podrán limitar la aplicación del apartado 1 del artículo 4, del artículo 11, del apartado 1 del artículo 12, de los artículos 13 a 17 y del apartado 1 del artículo 37 siempre y cuando tal limitación constituya una medida necesaria para:

… d) la seguridad nacional, el orden público y la defensa de los Estados miembros;"

En este tenor, se advierte que al existir dicha excepción se abre la posibilidad en que se exima de las obligaciones en el tratamiento de datos personales, por parte del responsable cuando se traten de circunstancias de seguridad nacional en uno o más de los Estados miembros.

Por otra parte, establece la figura del Supervisor Europeo de Protección de Datos, el cual será en el encargado de vigilar la protección de los datos personales en los países miembros (artículos 41 y 42).

Dicha figura es relevante, toda vez será la encargada de realizar la verificación de que el tratamiento de los datos personales se realice acorde a la normatividad de la materia, así como las transmisiones de datos, lo cual, en el caso que nos ocupa de los datos de los servidores públicos de instancias de seguridad nacional en nuestro país, ésta figura sería de mucho beneficio para la protección de datos personales.

1.6 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Este Reglamento establece las normas para el tratamiento de los datos personales y a la libre circulación de tales datos, asimismo, tiene aplicación al tratamiento total o parcial automatizado de los datos personales que se encuentren en un fichero (artículos 1 y 2).

De la misma manera, establece los principios a observar en el tratamiento como son la licitud, lealtad, transparencia, fines determinados, explícitos y legítimos, adecuados, pertinentes, limitados, exactos, limitación plazo de conservación, integridad y confidencialidad y responsabilidad proactiva (artículo 5).

Establece el tratamiento en diversas categorías de datos personales, donde se pueden determinar los diversos casos en los cuales algún titular de los datos puede exigir el cumplimiento (artículo 9).

Asimismo, se establece la información que debe facilitarse cuando los datos personales fueron obtenidos a través del titular de los datos, así como cuando los datos no se obtuvieron a través de éste (artículos 13 y 14).

En este Reglamento se establece el derecho de rectificación; el derecho a la supresión o como comúnmente se conoce el derecho al olvido; el derecho a la limitación del tratamiento; derecho de portabilidad de datos, así como el derecho a oposición (artículos 16, 17, 18, 20 y 21).

Dentro del Reglamento hace la aparición el Delegado de Protección de Datos, quien entre otras funciones supervisará el cumplimiento del ordenamiento legal en comento de la Unión Europea o de los Estados miembros (artículo 39).

De lo anterior, tenemos que una vez analizada la normatividad internacional, que pudiera ser aplicable al caso que nos ocupa, tenemos que las injerencias en la vida personal de toda persona, deben estar limitadas, ya que aún y cuando se

encuentren reguladas en diversas normatividades, debe haber un estricto control en cuanto al origen de los datos, es decir que éstos sean obtenidos de manera lícita, deben estar plenamente identificados los ficheros tanto físicos, así como electrónicos, asimismo, deben estar únicamente para el propósito que fueron recolectados y que éste propósito debe tener una temporalidad, la cual a su vencimiento deben ser notificados a las personas que los mismos serán destruidos.

Por lo cual, México al estar adherido al “Convenio 108 para la Protección de las Personas con respecto al tratamiento automatizado de los datos de carácter personal”, debe acatar dichas disposiciones y establecerlo como parte de la protección de datos personales, lo cual no acontece así de manera óptima ya que en el caso de los servidores públicos que laboran en instancias de seguridad nacional, no se precisan una vez recolectados los lugares a los cuales serán transferidos y mucho menos se realiza un aviso del momento en el que se van a destruir los datos que en su momento fueron recolectados.

De todo lo anteriormente analizado, podemos concluir que la protección de datos personales es un tema que ha ido evolucionando a través de los años en los diversos países a través de la normativa tanto de carácter internacional, así como en lo particular sobre todo en los países Europeos, los cuales han establecido de manera clara y precisa las reglas de su tratamiento.

En dichos países se han establecido los límites de la actuación del Estado en cuanto a la privacidad de las personas, lo cual repercute que las personas se encuentren protegidas por la normatividad en caso del mal uso de los datos personales.

Sin embargo, al igual que en nuestro país no se realiza precisión sobre el manejo de los datos personales del personal que labora en instancias de seguridad nacional, situación que debiera ser clarificada a efecto de tener certeza de del tratamiento de los datos personales.

En este tenor, México no ha quedado exceptuado de dicha evolución y ha emitido diversa normatividad en materia de protección de datos personales, las cuales han establecido la precisión de datos personales, las instituciones que vigilarán su protección, así como la manera en que serán tratados los mismos, como lo veremos en el siguiente capítulo.

Capítulo 2.

La Protección de Datos Personales en México

Capítulo 2. La Protección de Datos Personales en México

La protección de datos personales es un tema que ha ido evolucionando a nivel internacional con la promulgación de diversa normatividad, particularmente en Europa la cual ha enfocado sus esfuerzos en dicha protección.

De esta manera, México no siendo ajeno a dicho tema promulgó diversa normatividad de materia de acceso a la información y protección de datos personales, la cual lógicamente con el paso del tiempo ha ido evolucionando.

Asimismo, con la adhesión al Convenio 108 para la Protección de las Personas con respecto al tratamiento automatizado de los datos de carácter "personal", confirmó su compromiso con la protección de los datos personales, como a veremos en el presente capítulo.

2.1 Breve semblanza de los Datos Personales en México

El establecimiento del tema de protección de datos personales hizo su primera aparición en la legislación mexicana el 11 de junio año de 2002, con la publicación en el Diario Oficial de la Federación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. En esta ley no sólo se incorporaba la obligación por parte del gobierno mexicano de cumplir con diversas obligaciones de transparencia y de acceso a la información en poder de las instituciones del Estado, sino que también incorpora los datos personales y el tratamiento que se le debía dar a éstos. Siendo que a partir de ese momento se definen que son los datos personales y el alcance de los mismos.

Dicha Ley establece lo que se debe entender como datos personales, que en palabras de la autora Romina Garrido Iglesias "la protección de datos personales es la facultad de control de la información personal sobre su uso y destino, con el propósito de impedir que su circulación lesione los derechos de las personas",[24]

[24] Garrido Iglesias, Romina, 2015, *"La seguridad en el tratamiento de datos personales"*, en Reyes Olmedo, Patricia (coord.), *Ciudadanas 2020 III*, Chile p.77

situación que otorga al titular de los datos personales el reconocimiento, así como la protección de éstos.

La Ley referida dio origen al Instituto Federal de Acceso a la Información Pública Gubernamental, el cual era el órgano garante del acceso a la información pública, así como a la protección de datos personales.

Esta Ley incorporaba, entre otros, como parte de las obligaciones de transparencia el hacer público la estructura orgánica de la dependencia o entidad, así como sus facultades, el directorio de los servidores públicos los datos de los servidores públicos en funciones tales como su nivel presupuestal, salario y datos de contacto, domicilio de la Unidad de Enlace, los trámites que se ofrecen, la información del presupuesto asignado, las concesiones y los contratos asignados, las obras públicas realizadas, entre otros, lo cual fue el inicio del acceso a la información bajo el amparo de la ley de la materia (artículo 7). [25]

[25] **Artículo 7.** Con excepción de la información reservada o confidencial prevista en esta Ley, los sujetos obligados deberán poner a disposición del público y actualizar, en los términos del Reglamento y los lineamientos que expida el Instituto o la instancia equivalente a que se refiere el Artículo 61, entre otra, la información siguiente:
I. Su estructura orgánica;
II. Las facultades de cada unidad administrativa;
III. El directorio de servidores públicos, desde el nivel de jefe de departamento o sus equivalentes;
IV. La remuneración mensual por puesto, incluso el sistema de compensación, según lo establezcan las disposiciones correspondientes;
V. El domicilio de la unidad de enlace, además de la dirección electrónica donde podrán recibirse las solicitudes para obtener la información;
VI. Las metas y objetivos de las unidades administrativas de conformidad con sus programas operativos;
VII. Los servicios que ofrecen;
VIII. Los tramites, requisitos y formatos. En caso de que se encuentren inscritos en el Registro Federal de Tramites y Servicios o en el Registro que para la materia fiscal establezca la Secretaría de Hacienda y Crédito Público, deberán publicarse tal y como se registraron;
IX. La información sobre el presupuesto asignado, así como los informes sobre su ejecución, en los términos que establezca el Presupuesto de Egresos de la Federación. En el caso del Ejecutivo Federal, dicha información será proporcionada respecto de cada dependencia y entidad por la Secretaría de Hacienda y Crédito Público, la que además informará sobre la situación económica, las finanzas y la deuda públicas, en los términos que establezca el propio presupuesto;
X. Los resultados de las auditorias al ejercicio presupuestal de cada sujeto obligado que realicen, según corresponda, la Secretaría de la Función Pública, las contralorías internas o la Auditoría Superior de la Federación y, en su caso, las aclaraciones que correspondan;
XI. El diseño, ejecución, montos asignados y criterios de acceso a los programas de subsidio. Así como los padrones de beneficiarios de los programas sociales que establezca el Decreto del Presupuesto de Egresos de la Federación;
XII. Las concesiones, permisos o autorizaciones otorgados, especificando los titulares de aquéllos;

En el artículo 3, fracción segunda de la aducida Ley se establece lo siguiente:

*"**Artículo 3.** Para los efectos de esta Ley se entenderá por: …*

***II. Datos personales:** Cualquier información concerniente a una persona física identificada o identificable;"*.

En el Capítulo IV de la mencionada Ley, denominado "Protección de datos personales", se estableció lo siguiente:

***"Artículo 20.** Los sujetos obligados serán responsables de los datos personales y, en relación con estos, deberán:*

I. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, de conformidad con los lineamientos que al respecto establezca el Instituto o las instancias equivalentes previstas en el Artículo 61;"

En este artículo podemos observar que se establecen los principios de acceso y corrección de datos personales, de toda persona que haya almacenado sus datos personales en las bases de datos de los responsables del tratamiento.

Por otra parte, en el mismo artículo fracción III, establecía que se deberá poner a disposición de los individuos los propósitos de recolección de los datos personales (Aviso de privacidad), el cual a continuación se reproduce.

XIII. Las contrataciones que se hayan celebrado en términos de la legislación aplicable detallando por cada contrato:
a) Las obras públicas, los bienes adquiridos, arrendados y los servicios contratados; en el caso de estudios o investigaciones deberá señalarse el tema específico;
b)El monto;
c) El nombre del proveedor, contratista o de la persona física o moral con quienes se haya celebrado el contrato, y
d) Los plazos de cumplimiento de los contratos;
XIV. El marco normativo aplicable a cada sujeto obligado;
XV. Los informes que, por disposición legal, generen los sujetos obligados;
XVI. En su caso, los mecanismos de participación ciudadana, y
XVII. Cualquier otra información que sea de utilidad o se considere relevante, además de la que con base a la información estadística, responda a las preguntas hechas con más frecuencia por el público.
La información a que se refiere este Artículo deberá publicarse de tal forma que facilite su uso y comprensión por las personas, y que permita asegurar su calidad, veracidad, oportunidad y confiabilidad. Las dependencias y entidades deberán atender las recomendaciones que al respecto expida el Instituto.

"Artículo 20 …

… III. Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61…"

Para el caso que nos ocupa, en su momento no fue llevado a cabo para el caso de los servidores públicos en instancias de seguridad nacional como el Instituto Nacional de Migración, toda vez que al ingresar no se les informaba de manera precisa los datos a dónde iban a ser canalizados con la justificación de que en términos de la Ley de la materia cuando se transmita información a los Órganos de la Administración Pública Federal, no se requería del consentimiento expreso.

Asimismo, el artículo 22, en su fracción III establecía que "no se requeriría el consentimiento de los individuos para proporcionar los datos personales, cuando fueran transmitidos entre sujetos obligados o entre dependencias y entidades, siempre y cuando se utilizaren para el ejercicio de facultades propias, es decir, si estaba dentro de las atribuciones de cualquier sujeto obligado."

En complemento a la Ley de Transparencia citada, el 30 de septiembre de 2005 se publicaron en el Diario Oficial de la Federación, los Lineamientos de Protección de Datos Personales, los cuales en su lineamiento 1º establecía como objeto lo siguiente:

"Primero. Los presentes lineamientos tienen por objeto establecer las políticas generales y procedimientos que deberán observar las dependencias y entidades de la Administración Pública Federal para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales con el propósito de asegurar su adecuado tratamiento e impedir si transmisión ilícita y lesiva para la dignidad y derechos del afectado."[26]

Como podemos observar al igual que la Ley de Transparencia el ámbito de aplicación sólo era a nivel de la Administración Pública Federal, y buscaba

[26] Instituto Nacional de Acceso a la Información, en http://inicio.inai.org.mx/MarcoNormativoDocumentos/lineamientos_protdaper.pdf (consultada el 21 de septiembre de 2018).

establecer las políticas generales para el uso y destino de los datos personales que estuvieran en posesión de los órganos del poder Ejecutivo. Sin embargo, la protección era a nivel parcial ya que los poderes Legislativo y Judicial quedaban fuera del alcance de aplicación de la Ley.

Asimismo, en su lineamiento Quinto, establecía que, en el tratamiento de los datos personales, las dependencias y entidades debían observar los principios de licitud, calidad, acceso, seguridad, custodia y consentimiento para su transmisión.

En el mismo orden de ideas, en su Capítulo IV denominado “De la transmisión”, establecía que en términos de lo establecido por el artículo 22 de la Ley de Transparencia citada, podía realizarse la transmisión sin el consentimiento del titular de los datos.

> **“Artículo 22.** No se requerirá el consentimiento de los individuos para proporcionar los datos personales en los siguientes casos:
>
> **I.** Los necesarios para la prevención o el diagnóstico médico, la prestación de asistencia médica o la gestión de servicios de salud y no pueda recabarse su autorización;
>
> **II.** Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;
>
> **III.** Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;
>
> **IV.** Cuando exista una orden judicial;
>
> **V.** A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido, y
>
> **VI.** En los demás casos que establezcan las leyes.”

Asimismo, podemos observar que no había precisión respecto de los servidores públicos, y mucho menos de aquellos que laboraban dentro de las instancias de seguridad nacional.

Como podemos observar en dicha Ley, así como en los lineamientos no se precisó el caso de los servidores públicos que laboraran en una instancia de seguridad nacional, por tanto, dicho punto quedó de manera general para que se aplicara de manera genérica.

Por otro lado, la mencionada normatividad únicamente establecía que los datos personales se pondrían a disposición de la gente a través de las páginas web, en este caso, es el primer acercamiento hacia la transferencia de datos personales por medios electrónicos, sin embargo, no se precisó de qué manera se iban a compartir los datos, si era sólo de manera física o de manera digital.

El 1 de junio el año 2009 se reformó la Constitución Política de los Estados Unidos Mexicanos, adicionando un párrafo al artículo 16, estableciendo la protección de los datos personales como derecho fundamental y autónomo, quedando de la siguiente manera:

> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.[27]

De lo anterior, tenemos que se reconoció a nivel constitucional los derechos de acceso, rectificación, cancelación y manifestar oposición respecto de los datos personales. Es decir, los denominados derechos ARCO se establecieron como una garantía más para cualquier persona.

El 5 de julio de 2010, se publicó en el Diario Oficial de la Federación la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, la cual

[27] Diario Oficial de la Federación, en http://dof.gob.mx/nota_detalle.php?codigo=5092143&fecha=01/06/2009 (consultada el 21 de septiembre de 2018).

tiene como objeto proteger los datos personales que estén en posesión de los particulares.

Con esta ley se busca regular el tratamiento de los datos personales, así como garantizar a las personas el derecho que tienen de autodeterminación en la explotación de los datos personales. Dicha ley es aplicable a las personas físicas o morales privadas que reciban y realicen tratamiento de datos, dejando excluidas a las Sociedades de información crediticia, como a las que no sean realizadas para divulgación o utilización comercial (Artículo 2).[28]

En el año 2012, la Maestra Lina Ornelas Núñez, realizó un estudio comparativo respecto de la sintonía y coincidencias de la legislación Mexicana vigente la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, con normativas a nivel internacional, como es el caso de las Directrices de la OCDE, el Convenio 108, la Directiva 95/46/CE, la Resolución de Madrid y el Marco de privacidad APEC.[29]

[28] Articulo 2.- Son sujetos regulados por esta Ley, los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de:

I. Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y

II. Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

Se puede consultar en http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf
(consultada en 19 de septiembre de 2018)

[29] Ornelas Núñez, Lina, Curso Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento, Tirant Lo Blanch Formación. México 2012

Principio/Deber	LFPDPPP	Directrices de la OCDE	Convenio N° 108	Directivas 95/46/CE	Resolución de Madrid	Marco de privacidad APEC
Licitud	✓	✓	✓	✓	✓	✓
Consentimiento	✓	✓	✗	✓	✓	✓
Información	✓	✓	✓	✓	✓	✓
Calidad	✓	✓	✓	✓	✓	✓
Finalidad	✓	✓	✓	✓	✓	✓
Lealtad	✓	✓	✓	✓	✓	✓
Proporcionalidad	✓	✓	✓	✓	✓	✓
Responsabilidad	✓	✓	✗	✗	✓	✓
Seguridad	✓	✓	✓	✓	✓	✓
Confidencialidad	✓	✗	✗	✓	✓	✗

Cuadro comparativo Ley Federal de Protección de Datos Personales en Posesión de los Particulares, con normativas a nivel internacional.

Fuente. Ornelas Núñez Lina

Como se puede observar, en ese momento la Legislación Mexicana cumplía con los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad, responsabilidad, así como con los deberes de seguridad y confidencialidad. A diferencia de las otras como es el caso del Convenio 108 que no cumple con los principios de consentimiento, responsabilidad y confidencialidad, quedando con esto de manera más clara que aún y cuando solo se trataba de la protección de datos en posesión de particulares, se tenía una legislación que buscaba en todo momento proteger los datos de las personas que son tratados en territorio nacional.

2.1.1 Reforma Constitucional 2014

A los 7 días del mes de febrero de 2014, fue publicado en el Diario Oficial de la Federación el “Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos en materia de transparencia”.[30] En éste se adicionó al artículo 6, que el acceso a la información

[30] Diario Oficial de la Federación, en

involucra a todo ente administrativo en los ámbitos federales, estatales o municipales, de los tres poderes, así como "… órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal…"[31]. Asimismo, se estableció la creación del organismo autónomo quien sería el responsable de garantizar el acceso a la información y la protección de datos personales.

Derivado de esta reforma constitucional, en el Transitorio Segundo se estableció que el Congreso de la Unión expediría la ley relativa al artículo 6, por lo cual, deviene la publicación subsecuente de las leyes generales en materia de transparencia y protección de datos en posesión de sujetos obligados.

Algunos de los puntos relevantes de esta reforma es el hecho que el Órgano Garante contará con autonomía plena, ya que antes de la reforma sólo contaba con autonomía de gestión, lo cual implica total independencia a los poderes de la unión.

Por otra parte, se establece que las resoluciones del Órgano Garante serán definitivas e inatacables por parte de los sujetos obligados, a excepción del Consejero Jurídico de la Presidencia, el cual puede impugnarlas a través del Recurso de revisión, cuando se llegue a vulnerar la seguridad nacional. Este punto es muy importante, toda vez que ante una violación a la protección de datos personales por parte de algún sujeto obligado, el titular de los datos personales puede denunciar ante el Órgano Garante y éste aplicar las sanciones correspondientes.

---

https://dof.gob.mx/index_111.php?year=2014&month=02&day=07#gsc.tab=0 (consultada el 22 de septiembre de 2018)

[31] Diario Oficial de la Federación, en http://www.dof.gob.mx/nota_detalle.php?codigo=5332003&fecha=07/02/2014 (consultada el 22 de septiembre de 2018)

2.1.2 Ley General de Transparencia y Acceso a la Información Pública

El 4 de mayo de 2015, se publicó en el Diario Oficial de la Federación la Ley General de Transparencia y Acceso a la Información Pública, la cual en su artículo 1, segundo párrafo establecía lo siguiente: *"Tiene por objeto establecer los principios, bases generales y procedimientos para garantizar el derecho de acceso a la información en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad de la Federación, las Entidades Federativas y los municipios."* Esto es, el ámbito de aplicación es mucho más amplio que la ley antecesora en materia de transparencia y acceso a la información.

Asimismo, en el artículo 6 estableció el acceso a la información de cualquier entidad de los tres poderes de la unión, así como de los órganos autónomos, sindicatos que reciba fondos públicos y de partidos políticos.[32]

Dicha Ley en sus artículos 68 y 69 establece lo siguiente:

"Artículo 68. Los sujetos obligados serán responsables de los datos personales en su posesión y, en relación con estos, deberán:

I. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso, rectificación, corrección y oposición al tratamiento de datos, en los casos que sea procedente, así como capacitar a los Servidores Públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, de conformidad con la normatividad aplicable;

II. Tratar datos personales solo cuando estos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido

[32] Artículo 6 El Estado garantizará el efectivo acceso de toda persona a la información en posesión de cualquier entidad, autoridad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos; así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito de la Federación, de las Entidades Federativas y los municipios.

o dicho tratamiento se haga en ejercicio de las atribuciones conferidas por ley;

III. Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los propósitos para su tratamiento, en términos de la normatividad aplicable, excepto en casos en que el tratamiento de los datos se haga en ejercicio de las atribuciones conferidas por ley;

IV. Procurar que los datos personales sean exactos y actualizados;

V. Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación, y

VI. Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, perdida, transmisión y acceso no autorizado.

Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información de acuerdo a la normatividad aplicable. Lo anterior, sin perjuicio a lo establecido por el artículo 120 de esta Ley."

"Articulo 69. Los particulares, sin perjuicio de que sean considerados sujetos obligados de conformidad con la presente Ley, serán responsables de los datos personales de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares."

Como podemos observar, se establece en dicha Ley la obligación de los sujetos obligados de adoptar los procedimientos adecuados para el ejercicio de los Derechos ARCO. Asimismo, establece que los datos personales recabados solo podrán ser tratados cuando no sean excesivos con respecto del propósito para los cuales fueron obtenidos conforme a las atribuciones por la ley.

En este artículo se establece de manera expresa que los sujetos obligados no pueden distribuir los datos personales que se encuentren en los sistemas de información, salvo que exista manifestación expresa de los titulares de los datos, siendo esta disposición aplicable a las personas que laboran o que hayan laborado en alguna instancia de seguridad nacional.

Por otra parte, también establece que los particulares que sean considerados como sujetos obligados por esta Ley, deberán ser responsables de los datos personales que recaben en términos de su ordenamiento aplicable, como es el caso de los partidos políticos, los cuales recaban datos personales de los afiliados.

Esta Ley en su artículo Segundo Transitorio estableció lo siguiente: *"Segundo:*

Queda derogada cualquier disposición que contravenga los principios, bases, procedimientos y derechos reconocidos en la presente Ley, sin perjuicio de lo previsto en los siguientes Transitorios"; esto es derogó lo relacionado con la materia de transparencia y acceso a la información que se establecía en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental."

De esta manera tenemos, que con esta Ley tienen la obligación de proteger los datos personales los poderes Ejecutivo, Legislativo y Judicial, así como los sindicatos, partidos políticos y órganos autónomos, los cuales deberán de cumplir con los principios rectores de dicha protección. Dicha obligación se encuentra concatenada con las obligaciones establecidas en la LGPDPPSO, y que debiere ser aplicable en la protección de datos de los servidores públicos de instancias de seguridad nacional.

2.1.3 Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

El 26 de enero de 2017, se publicó en el Diario Oficial de la Federación la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la cual en su artículo 1, cuarto párrafo establece el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados.

Artículo 1. *La presente Ley es de orden público y de observancia general en toda la República, reglamentaria de los artículos 6o., Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, en materia de protección de datos personales en posesión de sujetos obligados.*

Todas las disposiciones de esta Ley General, según corresponda, y en el ámbito de su competencia, son de aplicación y observancia directa para los sujetos obligados pertenecientes al orden federal.

El Instituto ejercerá las atribuciones y facultades que le otorga esta Ley, independientemente de las otorgadas en las demás disposiciones aplicables.

Tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados.

Son sujetos obligados por esta Ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

A diferencia de las anteriores legislaciones en materia de datos personales, esta tiene aplicación no sólo para el gobierno federal, sino que es aplicable para los Poderes Ejecutivo, Legislativo y Judicial a nivel federal, estatal y municipal, incluyendo los órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

Es decir, su ámbito de aplicación es para cualquier órgano de los poderes ejecutivo, legislativo y judicial, del ámbito federal, estatal y municipal, lo cual de manera general es paso muy importante, ya que de esta manera se homologa la protección de datos personales.

En el artículo 3 de la citada ley, se realizan diversas definiciones que a continuación se exponen:

"Artículo 3. *Para los efectos de la presente Ley se entenderá por:*

II. ***Aviso de privacidad:*** *Documento a disposición del titular de forma física, electrónica o en cualquier formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos;*

VIII. Consentimiento: *Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos;*

IX. Datos personales: *Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;*

X. Datos personales sensibles: *Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;*

XI. Derechos ARCO: *Los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales;*

XXXII. Transferencia: *Toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado;*

XXXIII. Tratamiento: *Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales, y"*

Como se puede observar, la ley precisa diversos conceptos esenciales en el ámbito de la protección de datos personales tales como el consentimiento que es sin duda de los aspectos más importantes al definirlo como la "*Manifestación de la voluntad libre, específica e informada del titular de los datos mediante la cual se efectúa el tratamiento de los mismos*". (Artículo 3, fracc. VIII)

Asimismo, en las fracciones IX y X, del citado artículo 3, tenemos otros relevantes como los datos personales y datos sensibles; siendo los primeros "cualquier información concerniente a una persona física identificada o identificable", haciendo la acotación que una persona es identificable cuando la entidad de ésta puede ser conocida directa o indirectamente a través de cualquier información.

En el caso de los datos sensibles refiere a los de la esfera más íntima de su titular, entre otros menciona estado de salud, creencias religiosas y morales, así

como la preferencia sexual, por lo que, en palabras de Mariano Rosales Ortiz, los datos sensibles los define como los "que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste".[33]

En este tenor, tenemos que la información asociada de una persona es la que solo por conocer esa información puede conocerse la identidad del titular de los datos, siendo que, en el caso de la información no asociada, es la que sólo se conoce de manera aislada ciertos datos de las personas sin llegar a identificar al individuo, por lo que sería necesario el procesamiento de los datos con los que se cuente para conocer la identidad.

En términos de lo establecido en su artículo 14, establece diversas atribuciones del Sistema Nacional de Transparencia, entre la que destaca la fracción IX. Diseñar e implementar políticas en materia de protección de datos personales; esto es, en materia de protección de datos será el que establezca las políticas generales.

De lo anterior, se observa que tanto en la Ley General de Transparencia y Acceso a la Información Pública y en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se establecen diversas obligaciones de Transparencia, en las cuales de acuerdo a la naturaleza de la ley se establecen diversas acciones, existiendo el algún punto similitudes o igualdad entre los puntos, como a continuación veremos:

Artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública, establece lo siguiente:

"Obligaciones de los sujetos obligados: Poner a disposición del público y mantengan actualizada, en los respectivos medios electrónicos, de acuerdo con sus facultades,

[33] Rosales Ortiz, Mariano Carlos, *Prontuario de protección de datos personales*, Aqua Ediciones, México, 2016, p. 169.

atribuciones, funciones u objeto social, según corresponda, la información, por lo menos, de los temas, documentos y políticas siguientes:[34]

"Artículo 71 de la Ley General de Transparencia y Acceso a la Información Pública, establece lo siguiente:

En el caso del **Poder Ejecutivo Federal**, los poderes ejecutivos de las Entidades Federativas, el Órgano Ejecutivo del Distrito Federal y los municipios:

[34] VII. Directorio de todos los Servidores Públicos, a partir del nivel de jefe de departamento o su equivalente, o de menor nivel, cuando se brinde atención al público, manejen o apliquen recursos públicos, realicen actos de autoridad o presten servicios profesionales bajo el régimen de confianza u honorarios y personal de base. El directorio deberá incluir el nombre, cargo o nombramiento asignado, nivel del puesto en la estructura orgánica, fecha de alta en el cargo, número telefónico, domicilio para recibir correspondencia, correo electrónico oficial.
VIII. Remuneración bruta y neta de todos los Servidores Públicos de base o confianza, de todas las percepciones, incluyendo sueldos, prestaciones, gratificaciones, primas, comisiones, dietas, bonos, estímulos, ingresos y sistemas de compensación, señalando la periodicidad de dicha remuneración.
IX. Gastos de representación y viáticos, así como el objeto e informe de comisión correspondiente.
XI. Contrataciones de servicios profesionales por honorarios, señalando los nombres de los prestadores de servicios, los servicios contratados, el monto de los honorarios y el periodo de contratación.
XII. La información en Versión Pública de las declaraciones patrimoniales de los Servidores Públicos que así lo determinen
XIV. Convocatorias a concursos para ocupar cargos públicos y los resultados.
XV. Información de los programas de subsidios, estímulos y apoyos, en el que se deberá informar respecto de los programas de transferencia, de servicios, de infraestructura social y de subsidio.
XVII. La información curricular, desde el nivel de jefe de departamento o equivalente, hasta el titular del sujeto obligado, así como, en su caso, las sanciones administrativas de que haya sido objeto.
XVIII. El listado de Servidores Públicos con sanciones administrativas definitivas, especificando la causa de sanción y la disposición.
XIII. Los montos destinados a gastos relativos a comunicación social y publicidad oficial desglosada por tipo de medio, proveedores, número de contrato y concepto o campaña.
XXVI. Los montos, criterios, convocatorias y listado de personas físicas o morales a quienes, por cualquier motivo, se les asigne o permita usar recursos públicos o realicen actos de autoridad.
XXVII. Concesiones, contratos, convenios, permisos, licencias o autorizaciones otorgados, especificando los titulares de aquéllos, debiendo publicarse su objeto, nombre o razón social del titular, vigencia, tipo, términos, condiciones, monto y modificaciones, así como si el procedimiento involucra el aprovechamiento de bienes, servicios y/o recursos públicos.
XXXII. Padrón de proveedores y contratistas.
XXXVIII. Programas que ofrecen, incluyendo información sobre la población, objetivo y destino, así como los trámites, tiempos de respuesta, requisitos y formatos para acceder a los mismos.
XXIX Actas y resoluciones del Comité de Transparencia.
XLII. Listado de jubilados y pensionados y el monto que reciben.
XLIII. Ingresos recibidos por cualquier concepto señalando el nombre de los responsables de recibirlos, administrarlos y ejercerlos, así como su destino, indicando el destino de cada uno de ellos.
XLIV. Donaciones hechas a terceros en dinero o en especie.
XLVIII. Cualquier otra información que sea de utilidad o se considere relevante, además de la que, con base en la información estadística, responda a las preguntas hechas con más frecuencia por el público."

d) Nombre, denominación o razón social y clave del registro federal de los contribuyentes a los que se les hubiera cancelado o condonado algún crédito fiscal, así como los montos respectivos. Asimismo, la información estadística sobre las exenciones previstas en las disposiciones fiscales.

e) Nombres de las personas a quienes se les habilitó para ejercer como corredores y notarios públicos, así como sus datos de contacto, la información relacionada con el proceso de otorgamiento de la patente y las sanciones que se les hubieran aplicado."

"Artículo 79 de la Ley General de Transparencia y Acceso a la Información Pública, establece lo siguiente:

II. En el caso de los municipios el contenido de las gacetas municipales y las actas de sesiones de cabildo, los controles de asistencia de los integrantes del Ayuntamiento a las sesiones de cabildo y el sentido de votación de los miembros del cabildo sobre las iniciativas o acuerdos.

Los sindicatos que reciban y ejerzan recursos públicos deberán mantener actualizada y accesible, de forma impresa para consulta directa y en los respectivos sitios de Internet, adicionalmente lo siguiente:

II. Directorio del Comité Ejecutivo.

III. Padrón de socios.

Por lo que se refiere a los documentos que obran en el Expediente de registro de las asociaciones, únicamente estará clasificada como información confidencial, los domicilios de los trabajadores señalados en los padrones de socios.

Los sujetos obligados que asignen recursos públicos a los sindicatos, deberán habilitar un espacio en sus páginas de Internet para que éstos cumplan con sus obligaciones de transparencia y dispongan de la infraestructura tecnológica para el uso y acceso a la Plataforma Nacional. En todo momento el sindicato será el responsable de la publicación, actualización y accesibilidad de la información."

“Artículo 11 de la Ley Federal de Transparencia y Acceso a la Información Pública, establece lo siguiente:

Obligaciones de los sujetos obligados: deberán cumplir según corresponda, de acuerdo a su naturaleza, con las siguientes obligaciones:

X. Cumplir con las resoluciones emitidas por el Instituto en ejercicio de las facultades legales respectivas.

XI. Publicar y mantener actualizada la información relativa a las obligaciones de transparencia.

XII. Difundir proactivamente información de interés público.

XV. Dar atención a las recomendaciones del Instituto.

XVI. Las demás que resulten de la Ley General y demás normatividad aplicable.”

Artículo 68 de la Ley Federal de Transparencia y Acceso a la Información Pública.[35]

Artículo 69 de la Ley Federal de Transparencia y Acceso a la Información Pública, establece lo siguiente:

Los sujetos obligados del Poder Ejecutivo Federal, deberán poner a disposición del público y actualizar la siguiente información:[36]

[35] Los sujetos obligados en el ámbito federal deberán cumplir con las obligaciones de transparencia y poner a disposición del público y mantener actualizada, en los respectivos medios electrónicos, de acuerdo con sus facultades, atribuciones, funciones u objeto social, según corresponda, la información, por lo menos, de los temas, Documentos y políticas e información señalados en el Título Quinto de la Ley General (Artículo 70 de la LGTAIP). Al respecto, aquella información particular de la referida en el presente artículo que se ubique en alguno de los supuestos de clasificación señalados en los artículos 110 y 113 de la presente Ley no será objeto de la publicación a que se refiere este mismo artículo; salvo que pueda ser elaborada una versión pública. En todo caso se aplicará la prueba de daño a que se refiere el artículo 104 de la Ley General.

[36] II A las fuerzas armadas,

a) Las estadísticas sobre indultos, juicios en trámite, resoluciones ejecutorias, por delito, por grado de los sentenciados, por año y sentencias cumplidas; la estadística de las licencias de armas de fuego por tipo.

IV. En materia de población: número de centros penitenciarios o centros de tratamiento para adolescentes; estadística migratoria de entradas de extranjeros con legal estancia en México y condición de estancia, eventos de extranjeros presentados y devueltos; desagregada por sexo, grupo de edad y nacionalidad; estadística de los grupos de protección a migrantes, por acciones de atención.

“Art. 74 de la Ley Federal de Transparencia y Acceso a la Información Pública, establece lo siguiente:

Respecto de las obligaciones específicas que deberán cumplir las personas físicas o morales que reciben y ejercen recursos públicos o realicen actos de autoridad se estará a lo dispuesto en el Capítulo IV del Título Quinto de la Ley General.

VI. En materia de política exterior: El listado de asuntos de protección a mexicanos en el exterior; número de constancias de suscripción del Convenio a que hace referencia la fracción I del artículo 27 Constitucional para obtener concesiones para la exploración y explotación de minas y aguas en territorio nacional, indicando la entidad federativa y la nacionalidad del solicitante; el número de constancias de suscripción del Convenio a que hace referencia la fracción I del artículo 27 Constitucional para la adquisición de bienes inmuebles fuera de la zona restringida, indicando la entidad federativa y la nacionalidad del solicitante, así como el número de permisos otorgados para la constitución de fideicomisos, señalando la fiduciaria, nacionalidad del fideicomisario y la entidad federativa donde se localiza el inmueble; número de cartas de naturalización; determinaciones o resoluciones emitidas por órganos u organismos jurisdiccionales internacionales en los que México haya sido parte o haya intervenido; tratados internacionales celebrados y en vigor para México y, en su caso, los informes de los mecanismos de revisión de su implementación; Información estadística sobre candidaturas internacionales que el gobierno de México postule; informe sobre el desempeño de los representantes de México cuando presidan, encabecen o coordinen comisiones, consejos, comités, grupos de trabajo, asambleas, reuniones y conferencias de alto nivel, mecanismos ad hoc, o cualquier órgano dependiente y/o de carácter subsidiario de organismos internacionales y mecanismos multilaterales; votos, posicionamientos e iniciativas de México emitidos en el seno de organismos internacionales y mecanismos multilaterales, así como las declaraciones y resoluciones que hubieren propuesto o copatrocinado, una vez que el proceso de negociación haya finalizado; acuerdos interinstitucionales registrados ante la Secretaría de Relaciones Exteriores a los que hace referencia la Ley Sobre la Celebración de Tratados; y los acuerdos ejecutivos, memorandos de entendimiento, protocolos, cartas de intención y otros instrumentos que, sin adoptar la categoría de Tratados, suscriben representantes del gobierno federal con representantes de otros gobiernos mediante los cuales se adquieren compromisos jurídicamente vinculantes.
VIII. En materia de economía: lista de los aranceles vigentes; nombres de las personas a quienes se les habilitó para ejercer como corredores públicos, así como el domicilio de las corredurías públicas, los resultados del examen definitivo por los cuales se obtuvo la habilitación y las sanciones que se les hubieran aplicado; y la Información estadística sobre controversias resueltas en arbitraje internacional en materia de comercio exterior.
XI. En materia del sector educación y cultura: El Catálogo de los Centros de Trabajo de carácter educativo en la educación básica, media superior, superior, especial, inicial y formación para el trabajo incluyendo la información relativa a su situación geográfica, tipo de servicio que proporciona y estatus de operación; listado del personal que presta sus servicios en los sistemas de educación pública básica, tecnológica y de adultos, cuyas remuneraciones se cubren con cargo a recursos públicos federales; padrón de beneficiarios de las becas, así como los procedimientos y requisitos para obtenerlas; y el catálogo de museos.”

Los sindicatos que reciban y ejerzan recursos públicos deberán mantener actualizada y accesible, en los respectivos sitios de Internet, la información aplicable de los artículos 70 y 79 de la Ley General.

Los partidos políticos en el orden federal, las agrupaciones políticas nacionales y las personas constituidas en asociación civil creadas por los ciudadanos que pretendan postular su candidatura independiente, según corresponda, deberán, en lo conducente, poner a disposición del público y actualizar la información señalada en los artículos 70 y 76 de la Ley General".

"Art. 1 de la Ley General de Protección de Datos Personales en posesión de sujetos obligados, establece lo siguiente:

Son sujetos obligados por esta Ley, en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

Los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal serán responsables de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares."

"Art. 2 de la Ley General de Protección de Datos Personales en posesión de sujetos obligados, establece lo siguiente:

Uno de sus objetivos es: Proteger los datos personales en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, de la Federación, las Entidades Federativas y los municipios, con la finalidad de regular su debido tratamiento."

"Art. 10 de la Ley General de Protección de Datos Personales en posesión de sujetos obligados.

Creación del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el cual se conformará de acuerdo con lo establecido en la Ley General de Transparencia y Acceso a la Información Pública. En materia de protección de datos personales, dicho Sistema tiene como función coordinar y evaluar las acciones relativas a la política pública transversal de protección de datos personales, así como establecer e implementar criterios y lineamientos en la materia, de conformidad con lo señalado en la presente Ley, la Ley General de Transparencia y Acceso a la Información Pública y demás normatividad aplicable."

"Artículo 11 de la Ley General de Protección de Datos Personales en posesión de sujetos obligados, establece lo siguiente:

El Sistema Nacional contribuirá a mantener la plena vigencia del derecho a la protección de datos personales a nivel nacional, en los tres órdenes de gobierno."

"Artículo 14 de la Ley General de Protección de Datos Personales en posesión de sujetos obligados, establece las funciones del Sistema Nacional de Transparencia.[37]

[37] El Sistema Nacional, además de lo previsto en la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable, tendrá las siguientes funciones en materia de protección de datos personales:
I. Promover el ejercicio del derecho a la protección de datos personales en toda la República Mexicana;
II. Fomentar entre la sociedad una cultura de protección de los datos personales.
III. Analizar, opinar y proponer a las instancias facultadas para ello proyectos de reforma o modificación de la normativa en la materia.
IV. Acordar y establecer los mecanismos de coordinación que permitan la formulación y ejecución de instrumentos y políticas públicas integrales, sistemáticas, continuas y evaluables, tendentes a cumplir con los objetivos y fines del Sistema Nacional, de la presente Ley y demás disposiciones que resulten aplicables en la materia.
V. Emitir acuerdos y resoluciones generales para el funcionamiento del Sistema Nacional.
VI. Formular, establecer y ejecutar políticas generales en materia de protección de datos personales.
VII. Promover la coordinación efectiva de las instancias que integran el Sistema Nacional y dar seguimiento a las acciones que para tal efecto se establezcan.
VIII. Promover la homologación y desarrollo de los procedimientos previstos en la presente Ley y evaluar sus avances.
IX. Diseñar e implementar políticas en materia de protección de datos personales.
X. Establecer mecanismos eficaces para que la sociedad participe en los procesos de evaluación de las políticas y las instituciones integrantes del Sistema Nacional.
XI. Desarrollar proyectos comunes de alcance nacional para medir el cumplimiento y los avances de los responsables.

De lo anterior, tenemos que particularmente por lo que respecta al artículo 68 de la Ley Federal de Transparencia y Acceso a la Información Pública, establece que los sujetos obligados deberán cumplir con las obligaciones de transparencia, con excepción de lo establecido en los artículos 110 y 113 de dicha ley, el primero siendo relativo a la información reservada, y el segundo respecto de la información confidencial.

Ahora bien, en el Título Segundo de la citada Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, "Capítulo III De los Principios", establece en su artículo 16 los principios que se deberán observar en el tratamiento de los datos personales los responsables, mismo que a la letra dice:

> ***"Artículo 16.*** *El responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales."*

Asimismo, el artículo 18 de dicha Ley, establece lo siguiente:

XII. Suscribir convenios de colaboración que tengan por objeto coadyuvar al cumplimiento de los objetivos del Sistema Nacional y aquellos previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia.
XIII. Promover e implementar acciones para garantizar condiciones de accesibilidad para que los grupos vulnerables puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales.
XIV. Proponer códigos de buenas prácticas o modelos en materia de protección de datos personales.
XV. Promover la comunicación y coordinación con autoridades nacionales, federales, de los Estados, municipales, autoridades y organismos internacionales, con la finalidad de impulsar y fomentar los objetivos de la presente Ley.
XVI. Proponer acciones para vincular el Sistema Nacional con otros sistemas y programas nacionales, regionales o locales.
XVII. Promover e impulsar el ejercicio y tutela del derecho a la protección de datos personales, a través de la implementación, organización y operación de la Plataforma Nacional, a que se refiere la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable.
XVIII. Aprobar el Programa Nacional de Protección de Datos Personales al que se refiere el artículo 12 de esta Ley.
XIX. Expedir criterios adicionales para determinar los supuestos en los que se está ante un tratamiento intensivo o relevante de datos personales, de conformidad con lo dispuesto por los artículos 70 y 71 de esta Ley.
XX. Expedir las disposiciones administrativas necesarias para la valoración del contenido presentado por los sujetos obligados en la Evaluación de impacto en la protección de datos personales, a efecto de emitir las recomendaciones no vinculantes que correspondan.
XXI. Las demás que se establezcan en otras disposiciones en la materia para el funcionamiento del Sistema Nacional."

"Artículo 18. *Todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.*

El responsable podrá tratar datos personales para finalidades distintas a aquéllas establecidas en el aviso de privacidad, siempre y cuando cuente con atribuciones conferidas en la ley y medie el consentimiento del titular..."

En este tenor, se tiene que dicho artículo establece de manera precisa que el responsable podrá tratar los datos personales para fines distintos a los que señaló en su aviso de privacidad, bajo la tutela de las atribuciones que se encuentren conferidas en la legislación con el requisito sine qua non que exista el consentimiento del titular de estos datos.

Para efectos de la manifestación del titular de los datos, el artículo 20 de la Ley, establece la manera en cómo se otorgará dicha manifestación, estableciendo tres maneras de obtenerla:[38]

De lo anteriormente transcrito, es evidente que el consentimiento del titular de los datos para el tratamiento de los mismos, de manera general debe contener tres características para que pueda entenderse que el mismo es plenamente legal, es decir, debe ser libre, especifico e informado. Por lo cual, sino se cumpliere con alguno de estos requisitos dicho consentimiento no es legalmente válido.

Asimismo, el artículo 21, señala que "el consentimiento podrá manifestarse de forma expresa o tácita. Se deberá entender que el consentimiento es expreso

---

[38] ***Artículo 20.*** *Cuando no se actualicen algunas de las causales de excepción previstas en el artículo 22 de la presente Ley, el responsable deberá contar con el consentimiento previo del titular para el tratamiento de los datos personales, el cual deberá otorgarse de forma:*

I. *Libre: Sin que medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular;*

II. *Específica: Referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento, e*

III. *Informada: Que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales.*

En la obtención del consentimiento de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad declarada conforme a la ley, se estará a lo dispuesto en las reglas de representación previstas en la legislación civil que resulte aplicable.

cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología, siendo que de forma tácita se deberá entender cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario."

Por otra parte, el artículo 22 (anteriormente citado) establece "los casos de excepción de obtener el consentimiento del titular de los datos personales."

De lo anterior, podemos observar que la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, estableció de manera detallada la manera en que pueda hacerse el tratamiento de los datos personales de cualquier persona mediando manifestación expresa, así como los casos de excepción. Asimismo, del artículo transcrito no se hace mención sobre el tema de seguridad nacional y que no se deba solicitar la manifestación del titular de los datos para ser transferidos a otros lugares en los cuales puedan tratados dichos datos.

Es decir, para el caso que se analiza en caso de no existir la manifestación expresa del titular de los datos que labore o haya laborado en una instancia de seguridad nacional, y que éste no haya sido notificado en el aviso de privacidad que los datos serán transferidos a otras instancias, las transferencias de sus datos son contrarias a derecho.

Sin embargo, dicha legislación nunca establece de manera expresa la situación de los servidores públicos de cualquier órgano de los tres poderes, ya sea federal, estatal o municipal.

De esta manera, se deduce que estas reglas serán aplicables no sólo a las personas que entregue sus datos personales con los sujetos obligados, sino que también deberán ser aplicables a los servidores públicos que laboren dentro de algún órgano o institución gubernamental.

De todo lo anterior, tenemos que con la entrada en vigor de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, se precisó más a detalle el tema de la manifestación ya sea expresa o tácita respecto de la voluntad para la transferencia de datos a terceros, sin embargo, lo que no fue

precisado es el tema de los servidores públicos en particular los de las instancias en seguridad nacional, el cual quedó ausente por lo cual, deberían aplicarse las mismas reglas que para cualquier otra persona, sin tomar en consideración, que dicha calidad conlleva algunas problemáticas especiales.

Estas problemáticas especiales, conllevan en el hecho de la transferencia de datos personales a nivel nacional, o en caso de ser requerido a nivel internacional por el solo hecho de laborar en dichas instancias, lo cual, debiera ser notificado al titular de los datos para efectos del tratamiento de datos personales.

Asimismo, el tema de transferencias de datos por medios electrónicos solo es mencionado de manera muy general sin establecer la forma en que se realizará la misma, el tipo de resguardo que tendrán dichos datos personales almacenados en forma electrónica, así como su destrucción respectiva cuando llegara el momento, lo cual, vuelve a dejar la laguna respecto de los datos personales en medios electrónicos.

De lo expuesto, podemos concluir que México a partir del año 2002, ha promulgado diversas normatividades en las cuales se ha buscado la protección de los datos personales, así como el tratamiento de éstos.

Cabe destacar, que se inició con la protección únicamente del poder Ejecutivo y hoy en día se encuentran obligados a brindar dicha protección a los tres poderes de la unión, los órganos autónomos, los sindicatos, los partidos políticos, e inclusive los particulares, con lo cual podemos observar la evolución a través de los años en la visión de proteger los datos personales.

Sin embargo, el tema de protección de los datos personales de los servidores públicos que laboran en instancias de seguridad nacional, no es del todo claro, por lo cual se realizará un análisis de esta figura en el siguiente capítulo.

Capítulo 3.

Las Instancias de Seguridad Nacional. Ingreso, estadía y transferencia de datos personales a través de medios electrónicos

Capítulo 3. Las Instancias de Seguridad Nacional. Ingreso, estadía y transferencia de datos personales a través de medios electrónicos

Las instancias de seguridad nacional dentro de sus requisitos de ingreso establecen las pruebas de control y confianza, en las cuales los candidatos proporcionan diversos datos personales a la instancia a la cual pretenden ingresar.

La protección de datos personales por parte de las instancias de seguridad nacional es una obligación que deben cumplir de acuerdo con la normatividad que hemos expuesto con anterioridad.

El instituto Nacional de Migración, es considerada una instancia de seguridad nacional y en la cual el procedimiento es similar al de las otras instancias, por lo cual se explicará a detalle el tema particular, en el cual se analizará si se cumple o no con la protección de datos.

3.1 El Instituto Nacional de Migración como instancia de Seguridad Nacional

El 31 de enero de 2005, se publicó en el Diario Oficial de la Federación la Ley de Seguridad Nacional[39], la cual establecía en su artículo 3 lo que se entendía por Seguridad Nacional.

> *"Artículo 3.- Para efectos de esta Ley, por Seguridad Nacional se entienden las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, que conlleven a:*
>
> *I. La protección de la nación mexicana frente a las amenazas y riesgos que enfrente nuestro país;*
>
> *II. La preservación de la soberanía e independencia nacionales y la defensa del territorio;*

[39] Ley de Seguridad Nacional (2005), publica en el Diario Oficial de la Federación el 31 de enero de 2005. https://www.diputados.gob.mx/LeyesBiblio/pdf/LSN.pdf

III. *El mantenimiento del orden constitucional y el fortalecimiento de las instituciones democráticas de gobierno;*

IV. *El mantenimiento de la unidad de las partes integrantes de la Federación señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos;*

V. *La defensa legítima del Estado Mexicano respecto de otros Estados o sujetos de derecho internacional, y*

VI. *La preservación de la democracia, fundada en el desarrollo económico social y político del país y sus habitantes".*

En su artículo 9 se establece que "las instancias de Seguridad Nacional contarán con la estructura, organización y recursos que determinen las disposiciones que les den origen".[40]

Dentro del artículo 12 se menciona "quienes integran el Consejo de Seguridad Nacional dentro de los que se encuentran el Secretario de Gobernación".[41]

De la misma manera en el artículo 30 de la citada ley, se establece que la información solo podrá ser recabada y procesada, entre otros para fines de Seguridad Nacional, al tenor siguiente: *"Artículo 30.- La información sólo podrá ser*

---

[40] Artículo 9.- Las instancias de Seguridad Nacional contarán con la estructura, organización y recursos que determinen las disposiciones que les den origen.

Las actividades propias de inteligencia para la Seguridad Nacional cuyas características requieran de confidencialidad y reserva para el éxito de las investigaciones serán normadas presupuestalmente de manera específica por las dependencias del Ejecutivo Federal que correspondan, de acuerdo con su competencia.

41 Artículo 12.- Para la coordinación de acciones orientadas a preservar la Seguridad Nacional se establece el Consejo de Seguridad Nacional, que estará integrado por:

I. El Titular del Ejecutivo Federal, quien lo presidirá;
II. El Secretario de Gobernación, quien fungirá como Secretario Ejecutivo;
III. El Secretario de la Defensa Nacional;
IV. El Secretario de Marina;
V. El Secretario de Seguridad Pública;
VI. El Secretario de Hacienda y Crédito Público;
VII. El Secretario de la Función Pública;
VIII. El Secretario de Relaciones Exteriores;
IX. El Secretario de Comunicaciones y Transportes;
X. El Procurador General de la República, y
XI. El Director General del Centro de Investigación y Seguridad Nacional.

Los integrantes del Consejo no podrán nombrar suplente. En caso de ausencia del Presidente, el Secretario Ejecutivo presidirá la reunión.

El Consejo contará con un Secretario Técnico, que será nombrado por el Presidente de la República, dependerá directamente de él, contará con un equipo técnico especializado y un presupuesto asignado en el Presupuesto de Egresos de la Federación. Este no será integrante del Consejo.

recabada, compilada, procesada y diseminada con fines de seguridad nacional por las instancias autorizadas."

En los artículos 50 y 51 de la Ley en comento, establecen que cada instancia es responsable de la información que se genere o que se custodie, en términos de la entonces vigente Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, agregando que fuera de lo establecido por ésta última ley, la información es reservada por motivos de seguridad nacional.

> *Artículo 50.- Cada instancia representada en el Consejo es responsable de la administración, protección, clasificación, desclasificación y acceso de la información que genere o custodie, en los términos de la presente Ley y de la Ley Federal de Transparencia y Acceso a la Información Pública gubernamental.*
>
> *Artículo 51.- Además de la información que satisfaga los criterios establecidos en la legislación general aplicable, es información reservada por motivos de seguridad nacional:*
>
> *I. Aquella cuya aplicación implique la revelación de normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipo útiles a la generación de inteligencia para la seguridad nacional, sin importar la naturaleza o el origen de los documentos que la consignen, o*
>
> *II. Aquella cuya revelación pueda ser utilizada para actualizar o potenciar una amenaza.*

Por otra parte, en los artículos 61, 62 y 63 de la citada Ley, se estableció el actuar de los servidores públicos dentro de las instancias de seguridad nacional, al determinar de manera expresa que en el ejercicio de sus funciones se preservará la legalidad, así como el respecto a los derechos fundamentales, los artículos son de la siguiente manera:

> *"Artículo 61.- Los servidores públicos cuyas áreas estén relacionadas con la seguridad nacional, orientarán, con base en los principios previstos en el artículo 3o., el desempeño de sus funciones, preservando los de legalidad, responsabilidad, respeto a los derechos*

fundamentales y garantías individuales y sociales, confidencialidad, lealtad, transparencia, eficiencia, coordinación y cooperación que deben cumplir en términos de las disposiciones legales que regulan al servicio público."

"Artículo 62.- Fuera de los casos y condiciones previstos por esta Ley, ninguna persona estará obligada a proporcionar información a los servidores públicos adscritos al Centro."

"Artículo 63.- Los datos personales de los sujetos que proporcionen información, serán confidenciales."

Es de tomar en consideración, que el artículo 63 establece que "los datos personales de los sujetos que entreguen a una instancia de seguridad nacional, serán confidenciales, lo cual respecto del trabajo que nos ocupa reafirma la hipótesis, toda vez que al ingresar en la instancia de seguridad nacional en particular al Instituto Nacional de Migración, se entregan datos personales, los cuales deben ser tratados por el Instituto de manera confidencial, siendo que los datos no pueden ser transferidos a otras instancias sin que exista la manifestación expresa por parte de su titular, lo cual no acontece el día de hoy."

En este sentido, debemos tomar en cuenta lo que mencionan los autores Hilda Nucci y Ernesto Villanueva al establecer "La relación de confianza entre el titular de los datos personales y el responsable permanece durante todo el tiempo en el responsable tiene los datos en su posesión."[42]

Por otra parte, el 18 de mayo de 2005, se publicó en el Diario Oficial de la Federación el Acuerdo por el que se reconoce al Instituto Nacional de Migración como instancia de seguridad nacional, dentro del cual se estableció lo siguiente:

ARTICULO PRIMERO. - El Consejo Nacional de seguridad nacional ha reconocido al Instituto Nacional de Migración como Instancia de seguridad nacional, por lo que sus bases de datos y sistemas de información que resulten pertinentes deberán integrar la Red Nacional de Información prevista en la Ley de seguridad nacional.

[42] Villanueva Ernesto, Nucci Hilda. Comentarios a la Ley Federal de Protección de datos Personales en Posesión de Particulares. México, Novum 2012, p.245

ARTICULO TERCERO. - A fin de instrumentar la Red Nacional de Información de seguridad nacional, el Instituto Nacional de Migración compartirá sus bases de datos y sistemas de información pertinentes y otorgará la cooperación técnica necesaria para que el Centro de Investigación y seguridad nacional tenga la posibilidad técnica de acceder directamente a dichos sistemas.

ARTICULO CUARTO. - La información que se obtenga del Instituto Nacional de Migración a partir del acceso, uso y manejo de las bases de datos a que se refiere el presente Acuerdo, sólo podrá ser recabada, compilada, procesada y diseminada con fines de seguridad nacional, en términos de lo dispuesto en el artículo 30 de la Ley de la materia y se sujetará a los principios de reserva contenidos en el mismo ordenamiento.

De lo anterior, podemos observar que estableció que la información que recopile el Instituto Nacional de Migración podría ser compartida con el entonces Centro de Inteligencia y seguridad nacional, para instrumentar la Red Nacional de Información de seguridad nacional.

Asimismo, se establece que la información que se obtenga del acceso y manejo de bases de datos del Instituto Nacional de Migración sólo podrá ser tratada con fines de seguridad nacional, lo cual eso incluye las bases de datos personales de los servidores públicos, los cuales deberán ser tratados con esa salvedad.

3.2 Proceso de selección e Ingreso.

El proceso de selección e ingreso al Instituto Nacional de Migración (INM), como tal conlleva a que el aspirante a servidor público deba cumplir con los requisitos establecidos para tal efecto.

Al ingresar como aspirante, en una primera etapa el individuo debe entregar documentación que contiene datos personales como: domicilio, estado civil, registro federal de contribuyentes (RFC), acta de nacimiento, CURP, comprobante de grado de estudios, para poder acreditar con todo esto que es un candidato viable para realizar las evaluaciones de ingreso a la institución.

Al realizar los exámenes correspondientes de control y confianza para acreditar que el individuo obtuvo los mejores resultados para ser seleccionado como miembro del Instituto Nacional de Migración, en los cuales todo aquél aspirante deba presentar datos personales y sensibles, así como información personal los cuales quedarán en manos del Instituto.

En relación al requisito y la valoración de los exámenes de control y confianza se hace la observación que si bien el Pleno de la Suprema Corte de Justicia de la Nación determinó que estos constituyen "instrumentos para acreditar" las cualidades que tiene la persona para permanecer en el servicio público. Siendo que los requisitos deben estar previstos en la Ley, como en este caso lo es la presentación de información personal. También lo es que la información que deriva de ellos constituye datos personales, incluso en su carácter de sensible. Toda vez que dentro de las pruebas que se llevan a cabo en estas evaluaciones se encuentran: las fisiológicas, para detectar el consumo de alguna droga lícita o ilícita lo cual, como ya se refirió, queda registrado en el expediente del individuo.

> ***EVALUACIONES DE CONTROL DE CONFIANZA. SON MEDIOS Y NO FINES EN SÍ MISMOS, Y SU CONSTITUCIONALIDAD DEPENDE DE LA VALIDEZ DEL REQUISITO LEGAL QUE PRETENDEN MEDIR.***
>
> *Las evaluaciones de **control** de **confianza** son instrumentos para acreditar que quienes se someten a ellas poseen ciertas cualidades para acceder o mantenerse en el ejercicio de alguna actividad dentro del servicio público, esto es, son medios y no fines en sí mismos. Por otra parte, los requisitos y calidades que debe reunir una persona para acceder a un cargo público o mantenerse en él deben estar previstos forzosamente en la ley, para que la eventual práctica de tales evaluaciones oficiales sean instrumentos válidos, útiles y razonables desde la perspectiva constitucional. Lo anterior significa que no son las evaluaciones de **control** de **confianza** las que pueden formar parte de los requisitos para acceder a un cargo público, sino aquellas condiciones para el acceso y ejercicio de determinados cargos y que puedan medirse con tales **exámenes**, lo cual estará sujeto al respeto de los derechos humanos garantizados en la Constitución Política de los Estados*

Unidos Mexicanos y en los tratados internacionales en los que el Estado Mexicano sea Parte.[43]

En el mismo tenor, el solicitante debe realizar pruebas fisiológicas para detectar el consumo de alguna droga lícita o ilícita.

Asimismo, se verifican evaluaciones patrimoniales, en cuanto a los ingresos y egresos de la persona de varios años atrás. Lo que incluye entre otros, una revisión exhaustiva de tarjetas de crédito, hábitos de consumo cotidiano, préstamos, adeudos, ingresos de cualquier índole, propiedades de bienes muebles e inmuebles, basándose en el historial proporcionado por el buró de crédito, así como cualquier otro de tipo de movimiento de manera informal que puede afectar el patrimonio de la persona. Lo cual se extiende a los familiares cercanos, referencias personales quedando nuevamente dicha información en el expediente de la persona solicitante a la vacante.

Aunado a lo anterior, se realiza la prueba de polígrafo, en la cual se hacen cuestionamientos de carácter personal, físico, hábitos, familiares, patrimoniales, conyugales, laborales, éticos, morales, entre otros, información que también queda registrada dentro del expediente de la persona solicitante.

El Instituto también efectúa una visita de inspección del hogar de la persona solicitante. La finalidad es verificar que los ingresos y egresos manifestados, sean coincidentes con lo declarado en el proceso, realizando diversos cuestionamientos de carácter personal, familiar, patrimonial y de hábitos de consumo y de vida, lo cual también queda asentado dentro del expediente.

Una vez realizados los exámenes de control y confianza, se obtienen los resultados de la evaluación del Centro de control y confianza respectivo, mismos que son registrados en el expediente del individuo. Aquí se determina si una persona es viable o no para ocupar el puesto en cuestión, siendo que, en caso positivo, elabora su alta respectiva. Para esto se agregan al expediente datos

[43] P./J. 12/2012, *Semanario Judicial de la Federación y su Gaceta*, Novena Época, Libro X, Julio de 2012, Tomo 1 Pág. 243

biométricos como: huellas dactilares, palma de la mano, del antemano, así como del iris de los ojos de la persona.

En este momento el candidato seleccionado lleva a cabo los trámites para el ingreso, entregando nuevamente información de carácter personal, a saber: domicilio, estado civil, edad, registro federal de contribuyentes, acta de nacimiento, CURP, constancias de estudios, datos bancarios, médicos, nombres de familiares, número de teléfono celular del aspirante como de familiares, entre otros.

En este punto la información que el servidor público ha entregado al Instituto es de carácter personal, laboral, financiera y familiar, siendo aquí el momento en el cual comienza la dispersión de la información del individuo.

En primer lugar, el Instituto Nacional de Migración integra un expediente del nuevo servidor público el cual es resguardado dentro del mismo. Se hace el reporte a la Secretaría de Gobernación, debido a que es un órgano desconcentrado. La misma Secretaría realiza el alta de la plaza presupuestal ocupada a la Secretaría de Hacienda y Crédito Público. A la cual se le otorga de manera sistematizada la información de la persona a efecto de realizar su registro correspondiente.

En este caso la Secretaría de Hacienda y Crédito Público conforma un expediente de manera electrónica del servidor público que ocupa la plaza presupuestal respectiva. Este contiene entre otra fecha de nacimiento, RFC, CURP, domicilio, correo electrónico personal, identificación oficial.

Por otro lado, la Secretaría de Gobernación realiza el alta respectiva por medios digitales ante Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE), a efecto de que el servidor público cuente con las prestaciones en materia de seguridad social. El ISSTE para poder llevar a cabo el expediente requiere el nombre, edad, domicilio, RFC, CURP, identificación oficial entre otros.

De aquí el ISSSTE, a su vez procede al alta del servidor público por medios digitales ante el Fondo de la Vivienda del ISSSTE (FOVISSSTE), para que se incorpore al nuevo servidor público en dicho sistema, requiriendo para esto de la

misma información y documentación que el ISSSTE solicitó para el alta, así como el monto de percepciones para poder realizar los cálculos respectivos.

Para este paso, la transferencia de datos personales por medios digitales sigue siendo de manera continua entre órganos de la Administración Pública Federal, haciendo expedientes en cada caso y teniendo el resguardo de los datos en cada lugar donde se depositan.

Aunado a lo anterior, el ingreso del ahora servidor público, sus datos personales, no sólo quedan registrados en el expediente, sino que también se envían por medios digitales a la base de datos de seguridad nacional denominada Plataforma México. Esta a su vez compartida con diversas agencias de inteligencia con las cuales México tiene acuerdos de compartir información en materia de seguridad nacional, como lo es la INTERPOL, la CIA y el FBI.

Dicha Plataforma México, se diseñó con el objeto de conjuntar la información en materia de seguridad pública de los tres órdenes de gobierno en nuestro país, lo cual incluye los datos de los servidores públicos que laboren en instancias de seguridad nacional.

En el Acuerdo 02/2007 del Secretario de Seguridad Pública, por el que se crean el Consejo Asesor y el Comité Técnico de la Plataforma México, publicado en el Diario Oficial de la Federación el 29 de marzo de 2007, establece dentro de los Considerandos que para el óptimo funcionamiento necesita entre las instancias de seguridad nacional *"…de la adopción de estrategias y del desarrollo de sistemas que la conformen y garanticen el adecuado intercambio de información, así como de soluciones de tecnologías de la información que permitan la interconexión exitosa de los múltiples sistemas y bases de datos existentes en el gobierno."*[44]

Como podemos observar, la información recopilada por la instancia de seguridad nacional no sólo es resguardada en el Instituto Nacional de Migración, sino que es compartida por medios digitales en Plataforma México. A la cual pueden

[44] Acuerdo 02/2007 del Secretario de Seguridad Pública, por el que se crean el Consejo Asesor y el Comité Técnico de la Plataforma México. Diario Oficial de la Federación 29 marzo de 2007. Se puede ver en: http://www.dof.gob.mx/nota_detalle.php?codigo=4966851&fecha=29/03/2007

tener acceso distintas instituciones internacionales. Lo que constituye una transferencia internacional de datos personales por medios digitales. Esto implica que dicha información no sólo es manejada dentro del territorio nacional, sino que es enviada a bases a la cual tienen acceso diversas instancias internacionales de seguridad.

De lo anterior, surge una interrogante a esta situación ¿si una persona ingresa dentro del servicio público en una instancia de seguridad nacional como lo es el Instituto Nacional de Migración, pierde el control de sus datos personales al realizarse diversas transferencias de sus datos por medios digitales sólo por el hecho de laborar en dicha instancia. De lo que ya vimos en primera instancia se contestaría que no, sin embargo, de acuerdo a lo que hemos visto resulta el caso de ser de esa manera, como a continuación veremos se explicará la pérdida del control de los datos personales por parte del titular.

La anterior interrogante, se hace por el motivo que, al ingresar a laborar en el servicio público particularmente en alguna instancia de seguridad nacional, los datos personales del individuo recorren un camino largo al ser dispersados y multiplicados para su tratamiento en diversos órganos de la Administración Pública Federal, sin que el titular conozca o sea informado explícitamente del camino que recorren los datos. Sin ser informado de la finalidad del tratamiento que se le darán en la instancia de seguridad nacional, el tiempo de resguardo de éstos una vez que terminan la relación laboral, el personal que tendrá acceso a los mismos, y sobre todo el tiempo que estarán resguardados dichos datos, lo cual viola los principios de información y finalidad, al no informar al titular de los datos la manera en que tratarán sus datos personales, así como al no respetar la finalidad para la cual fueron recabados.

Como un ejemplo de lo anterior, podemos comentar que, con la suscripción de la Carta de Acuerdo de la Iniciativa Mérida llevada a cabo entre los Estados Unidos de Norteamérica y México, para la cooperación bilateral en materia de seguridad nacional (2008), se establece realizar acciones conjuntas para combatir el crimen organizado. Como parte de esa cooperación se encuentra el compartir

datos personales de los individuos que trabajan en instancias de seguridad nacional a través de medios digitales.

Es por ello, que pareciera que el servidor público de la instancia de seguridad nacional como lo es el Instituto Nacional de Migración, se le restringe la protección de la legislación en materia de protección de datos personales, sólo por el hecho de ingresar al servicio público en estas instancias. Ya que no se le informa debidamente a éste la utilización de sus datos y las finalidades concretas y específicas en el tratamiento de los mismos para los que son compartidos por medios digitales a otros órganos. Lo que lleva a determinar, que los datos personales se encontrarán en diversos lugares sin que la persona tenga información concreta y explícita del tratamiento que se le den. Incluso en algunos casos los mismos pueden rebasar las fronteras de nuestro país y sean realizadas transferencias a otros países sin la protección adecuada de la legislación mexicana, excusando en causas de seguridad nacional.

Esto es así, ya que aún y cuando dicha actividad no se establece de manera expresa, al haber laborado en una instancia de seguridad nacional, en este caso el INM, tengo conocimiento que todos los datos personales de los trabajadores son compartidos entre ambos países (México-Estados Unidos de Norteamérica). Esto consideramos deja en estado de indefensión a los titulares de los datos ya que no se dan a conocer las transferencias por medios digitales, la manera en la que se manejan y protegen los datos, lo que puede ser distinta a la establecida en la legislación nacional, como más adelante se expone dicha situación.

Esta situación de la transferencia de datos sólo puede ser consultada por el personal que labore en dichas instancias de seguridad nacional y tenga acceso a dichos datos.

3.3 Transferencia de datos personales por parte del Instituto Nacional de Migración a otros entes gubernamentales.

Hasta entonces se podría mencionar que la transferencia de datos personales por medios digitales es acorde a lo establecido en la normatividad de la materia, debido

a que se ha realizado entre órganos gubernamentales y en el ejercicio de sus atribuciones.

Sin embargo, en este momento es cuando comienza una transferencia de datos personales por parte del Instituto Nacional de Migración por medios digitales que el servidor público desconoce. De manera general, al no informarle de manera concreta y explícita los órganos de gobierno por los cuales serán tratados.

En este tenor, es importante citar a Marcela I. Basterra, quien menciona que debe entenderse por "derecho a la protección de datos" a la suma de principios, derechos y garantías establecidos en favor de las personas que pudieran verse perjudicadas por el tratamiento de datos de carácter personal a ellas referidos".[45]

Es decir, estaríamos frente a lo que se conoce como la "vida privada" de las personas, la cual podemos tomar como referencia lo mencionado por los autores Gómez Robledo y Ornelas Núñez, que definen de la siguiente manera la vida privada *"Nosotros entendemos el concepto de "vida privada" como una idea muy extensa y genérica, que va a cubrir todo aquello que no deseamos llegue a ser parte del conocimiento general de una sociedad en particular. Ahora bien, dentro de la esfera de la vida privada, va a existir un núcleo que por lo general deseamos proteger con un empeño mucho mayor por considerarlo inseparable de la esencia misma de nuestra propia persona, y a éste lo entendemos como el concepto de intimidad"*.[46]

3.4 Ejemplo real de primera mano

Caso particular.

En el año 2011 ingresé a laborar al Instituto Nacional de Migración al puesto de Director de Transparencia. En ese momento, no me fue informado de manera concreta y explícita, los órganos de la Administración Pública Federal o en su caso, los órganos internacionales, a los cuáles iban a ser transferidos por medios digitales

[45] Basterra, Marcela I, "Protección de Datos Personales", Ediar EDRS, México 2008, p. 33.
[46] Gómez Robledo, Alfonso; Ornelas Núñez, Lina, "Protección de Datos Personales en México. El caso de Poder Ejecutivo en México", UNAM Instituto de investigaciones jurídicas, México 2003, p. 6.

mis datos personales, ni su almacenamiento, el tratamiento, el resguardo y las personas que tendrían acceso a los mismos.

En este supuesto se han violado los principios de finalidad, información y temporalidad al no tener conocimiento pleno de los órganos de la Administración Pública Federal y extraterritoriales a los cuales se les realizó la transferencia de mis datos.

Lo anterior, pudiese parecer un tema menor, sin embargo, ante un posible mal uso de mis datos personales, en primera instancia buscaría en los lugares en los cuales deposité los datos de manera inicial al momento del ingreso, verificando el tratamiento de los mismos, las personas que tuvieron acceso a los mismos y el espacio donde estuvieron resguardados, para poder determinar en su caso, las acciones legales que pudiera ejercer como titular de los datos, de acuerdo con el daño que se haya causado.

Sin embargo, al no ser el único lugar en el cual se encuentran resguardados mis datos personales, quedan más lugares en los cuáles se tienen acceso a los mismos y de los cuales no estoy informado, violando los principios referidos, ya que con la justificación de que se trata de transferencias de datos personales de manera oficial, se realiza de manera ajena a mi persona, lo cual se corroboró al realizar una solicitud de acceso a la información, la cual adelante expondremos.

De esta manera, al no tener conocimiento pleno del tratamiento que se les den a mis datos personales, e inclusive en algunos casos rebasando las fronteras del país, cuando son compartidos los datos en Plataforma México ¿cómo podría proteger el tratamiento que se le dan a los datos personales, sino se tiene la información de los lugares a los cuales se hayan transferido de manera electrónica?, violando de esta manera mi derecho fundamental de protección de datos personales, sólo por el hecho de tener la calidad de servidor público de una instancia de seguridad nacional como lo es el Instituto Nacional de Migración.

Cabe destacar, que la Declaración Universal de los Derechos Humanos, no realiza distinción alguna de que una persona por el hecho de tener alguna calidad

por razones de puesto o posición dentro del servicio público en cualquier país que haya reconocido dicho tratado internacional, queda exenta de la protección de la misma.

Siendo que, por ser servidor público en nuestro país dentro de la Administración Pública Federal en una instancia de seguridad nacional, exista una restricción de la protección del individuo en sus datos personales, sólo por el hecho de tener esta característica, al no poder tener conocimiento de los órganos gubernamentales que tienen acceso a los datos y el tratamiento de los mismos, a través de medios digitales

Lo anterior, se robustece con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la cual ha establecido expresamente la manera que pueden ser transferidos los datos personales en posesión de los sujetos obligados.

El artículo 16 de la mencionada Ley establece que el responsable de los datos deberá observar en su tratamiento los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad.[47]

Asimismo, el artículo 18 de la misma ley establece que todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera, lo cual se conoce como principio de finalidad.

El responsable podrá tratar datos personales para finalidades distintas a aquéllas establecidas en el aviso de privacidad, siempre y cuando cuente con atribuciones conferidas en la ley y medie el consentimiento del titular, salvo que sea una persona reportada como desaparecida, en los términos previstos en la presente

[47] Artículo 16. El responsable deberá observar los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales.

Ley y demás disposiciones que resulten aplicables en la materia, como es el caso de temas de transparencia.[48]

Siendo que el artículo 20 de la misma Ley, establece la manera en cómo se obtendrá el consentimiento previo del titular de los datos, tendiendo como características libre, específica e informada, siendo muy significativo lo establecido en la manera específica la cual es referida a finalidades concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento (artículo 18).

También es muy relevante lo establecido el principio de información, la cual se refiere a que el titular debe tener conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales, toda vez que al conocer el titular del tratamiento que se le darán a sus datos, tiene conocimiento cierto del destino de sus datos, y con esto no existe violación a su derecho. (Artículo 26)

De todo lo anterior, tenemos que en el caso de los servidores públicos de la instancia de seguridad nacional como lo es el Instituto Nacional de Migración es un caso sui generis, ya que la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados que tiene como garantizar el derecho que tiene toda persona a la protección de sus datos personales, debería de ser aplicable también a los servidores públicos de la misma manera. Sin embargo, no acontece así.

En este caso, vale la pena retomar lo establecido por el Convenio 108 del Consejo Europa del cual México es adherente, en el sentido de que las personas deben conocer la existencia del fichero automatizado que contiene sus datos personales, las finalidades principales de los datos, así́ como la identidad y la

---

[48] Artículo 18. Todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.

El responsable podrá tratar datos personales para finalidades distintas a aquéllas establecidas en el aviso de privacidad, siempre y cuando cuente con atribuciones conferidas en la ley y medie el consentimiento del titular, salvo que sea una persona reportada como desaparecida, en los términos previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia.

residencia habitual o el establecimiento principal de la autoridad controladora del fichero, señalando que cada determinado tiempo (intervalos razonables y sin demora o gastos excesivos) la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible (Artículo 8).

Este principio no fue retomado por la legislación mexicana, ya que no existe la obligación por parte de los sujetos obligados de confirmación de la existencia o no del fichero automatizado de datos personales que conciernan en este caso a un servidor público. Por lo cual, éste no sabe con exactitud cuando sus datos son destruidos o eliminados y la ubicación del lugar en dónde deberían ser destruidos.

Esto es así, toda vez que al momento de ingresar a trabajar una persona dentro del Instituto Nacional de Migración y requerirse diversa documentación, así como sus datos personales, se les hace del conocimiento mediante el aviso de privacidad, de manera general de diversos tratamientos que se les dará a sus datos, dependiendo el trámite a realizar, así como el reclamo de los derechos ARCO, entre otros.[49]

Sin embargo, del análisis a los diversos avisos de privacidad del INM, se advierte, que no existe algún aviso para el caso de los aspirantes o inclusive para los servidores públicos en activo, que se sometan a las evaluaciones del Centro de Control y Confianza. Por lo cual en este caso se violan los principios de licitud, finalidad y consentimiento.

En este caso, tenemos que el Instituto Nacional de Migración como instancia de seguridad nacional no informa al titular de los datos el tratamiento de sus datos cuando sean sometidos a exámenes de centro de control y confianza, y del expediente administrativo que se genere con la información general, así como en donde serán almacenados éstos, y en su caso, si se realizarán transferencias por

[49] Se pueden consultar en https://www.inm.gob.mx/gobmx/word/index.php/avisos-de-privacidad/ (consultado el 12 de diciembre de 2018)

medios digitales a otro Sujeto Obligado. Toda vez que se debería informar que los mismos son transferidos a otras instancias de seguridad nacional.

Luego entonces, el Instituto Nacional de Migración no respeta el derecho de protección de datos personales de manera óptima, ya que sigue las reglas de seguridad nacional, sin especificar el alcance de éstas dentro del tratamiento de los datos al no informarle esta situación al titular de los datos de manera concreta y explícita y no obtener el consentimiento expreso.

De lo anterior, mencionamos los 21 Avisos de Privacidad con los que cuenta el instituto Nacional de Migración, los cuales aparecen en su página de internet.

Dirección General de Regulación y Archivo Migratorio:

- ABTC para mexicanos.
- Sistema Electrónico de Trámites Migratorios (SETRAM) para empresas.
- Sistema Electrónico de Trámites Migratorios (SETRAM) para estancia.
- Sistema Electrónico de Trámites Migratorios (SETRAM) para internación.
- Centro de Atención Migratoria.

Dirección General de Control y Verificación Migratoria:

- Acuerdo Administrativo.
- Banco de datos de registro y control de denuncias.
- Acceso a Estaciones Migratorias y Estancias Provisionales.
- Procedimientos Administrativos Migratorios (PAM).
- Procedimientos de Revisión Migratoria.
- Procedimientos de Visitas de Verificación Migratoria.
- Sistema de Circuito Cerrado de TV (CCTV).
- Registro para los procesos de Internación y Salidas del Territorio Nacional Mexicano.
- Sistema de Información y Registro de Niñas, Niños y Adolescentes y Adultos Acompañantes (SIRENNA).

Dirección General de Protección al Migrante y Vinculación:

- Observador Paisano.
- Constancia de Recepción de Mexicanos Repatriados.
- Sistema de Análisis Paisano (SAPA).
- Sistema Integral de Operación Migratoria SIOM (módulo de repatriados).
- Base de datos de los grupos BETA.
- Emisión de cédula de entrevista a connacional repatriado (a).

Dirección General Jurídica, de Derechos Humanos y Transparencia:

- Módulo de Consultas Institucional (MCI).

Con el objeto de tener conocimiento del paradero de mis datos personales, procedí a realizar una solicitud de acceso a la información, en la cual se solicitó lo siguiente:

> *1. ¿Cuáles son los datos personales y sensibles que se tienen de mi persona en ese Instituto Nacional de Migración?*
>
> *2. ¿A qué Dependencia o Entidad de la Administración Pública Federal han sido transmitidos mis datos personales y sensibles?*
>
> *3. ¿A cuáles agencias internacionales de seguridad han sido transmitidos mis datos personales y sensibles, incluidos los datos biométricos?*
>
> *4. En relación con el numeral anterior, indique si fueron transmitidos mis datos personales y/o sensibles a la Plataforma México.*

Para lo cual recibí la siguiente respuesta:

SEGOB | INM

30 OCT 2018

17:01

SECRETARÍA DE GOBERNACIÓN.

INSTITUTO NACIONAL DE MIGRACIÓN.

DIRECCIÓN GENERAL DE ADMINISTRACIÓN.

DIRECCIÓN DE ADMINISTRACIÓN DE PERSONAL.

OFICIO No. INM/DGA/DAP/ 6553 **/2018.**

Ciudad de México, a 30 de octubre de 2018.

LIC. DAVID MAGAÑA MUÑOZ.
SUBDIRECTOR Y ENLACE TITULAR DE TRANSPARENCIA EN LA DIRECCIÓN GENERAL DE ADMINISTRACIÓN.
P R E S E N T E.

Hago referencia a su oficio INM/DGA/DGAAR/DNYC/STAOFMG/0855/2018, mediante el cual comunica que el Sistema de Atención de Solicitudes de Información (SASI) de este Instituto ha turnado a la Dirección General de Administración, la solicitud con número de folio 0411100124318, en el que solicita lo siguiente:

> *"C. [redacted], por medio del presente, y con fundamento en los artículos 1, 61, 122, 123, 124, 125, 135 y 136 de la Ley Federal de Transparencia y Acceso a la Información Pública, vengo a solicitar la siguiente información:*
> 1. *¿Cuáles son los datos personales y sensibles que se tienen de mi persona en ese Instituto Nacional de Migración?*
> 2. *¿A qué Dependencia o Entidad de la Administración Pública Federal han sido transmitido mis datos personales y sensibles?*
> 3. *¿A cuáles agencias internacionales de seguridad han sido transmitidos mis datos personales y sensibles, incluidos los datos biométricos?*
> 4. *En relación con el numeral anterior, indique si fueron transmitidos mis datos personales y/o sensibles a la Plataforma México.*
> ..." (Sic)

Al respecto, en atención a la información interés del solicitante, referente al numeral 1 de la petición, se hace de su conocimiento que en la Dirección de Administración de Personal de este Instituto se cuenta con el expediente único de personal del peticionario, mismo que contiene información concerniente a su persona, que lo hace identificado e identificable, directa e indirectamente, tales como su nombre, domicilio particular, sexo, estado civil, Registro Federal de Contribuyentes, Clave Única de Registro de Población, teléfono particular, número de empleado, huellas digitales, fotografía, ciudad de origen, edad, contiene además datos de su nacionalidad y del estado de salud que tenía en ese momento de la expedición del documento médico, información que pudiera llegar a ser sensible, datos personales que se refieren de manera enunciativa más no limitativa, es decir, que el expediente único de personal, en su cumulo contiene datos personales que también en determinado momento pudieran llegar a ser sensibles.

Ahora bien, en atención al numeral 2 de su petición se informa que se han trasmitidos datos personales a la Secretaría de Gobernación, en virtud de que el Instituto Nacional de Migración es un órgano administrativo desconcentrado dependiente de esta Secretaría, de conformidad con lo dispuesto en los artículos 17 de la Ley Orgánica de la Administración Pública Federal, 2 inciso C, fracción III y 54 del Reglamento Interior de la Secretaría de Gobernación.

En atención al numeral 3 de la solicitud de mérito, de la búsqueda exhaustiva realizada en los archivos y registros con que cuenta esta Dirección, así como del análisis pormenorizado realizado al expediente único de personal del peticionario, no se desprende información relativa a haber sido transmitidos datos personales y sensibles, incluidos los datos biométricos a agencias internacionales de seguridad.

1

SEGOB | SECRETARÍA DE GOBERNACIÓN INM INSTITUTO NACIONAL DE MIGRACIÓN

SECRETARÍA DE GOBERNACIÓN.

INSTITUTO NACIONAL DE MIGRACIÓN.

DIRECCIÓN GENERAL DE ADMINISTRACIÓN.

DIRECCIÓN DE ADMINISTRACIÓN DE PERSONAL.

OFICIO No. INM/DGA/DAP/ 6553 /2018.

Por último, referente al numeral 4 de la solicitud que nos ocupa, hago de su conocimiento que si han sido transmitidos datos personales y/o sensibles a la Plataforma México, de conformidad con el *"ACUERDO por el que se reconoce al Instituto Nacional de Migración como Instancia de Seguridad Nacional"*, publicado en el Diario Oficial de la Federación el 18 de mayo de 2005, así como en lo establecido por los artículos 122 y 123 de la Ley General del Sistema Nacional de Seguridad Pública, donde el personal de este Instituto es susceptible del registro y actualización en el *"Registro Nacional de Personal de Seguridad Pública"*, mismo que contendrá la información actualizada, relativa a los integrantes de las Instituciones, en este caso, de la Federación, el cual tendrá, por lo menos: los datos que permitan identificar plenamente y localizar al servidor público, sus huellas digitales, fotografía, escolaridad y antecedentes en el servicio, así como su trayectoria en la seguridad pública, los estímulos, reconocimientos y sanciones a que se haya hecho acreedor el servidor público, y cualquier cambio de adscripción, actividad o rango del servidor público, así como las razones que lo motivaron.

Sin otro particular, aprovecho la ocasión para enviarle un cordial saludo.

ATENTAMENTE.
EL DIRECTOR.

SECRETARÍA DE GOBERNACIÓN INM INSTITUTO NACIONAL DE MIGRACIÓN
DIRECCIÓN GENERAL DE ADMINISTRACIÓN
DIRECCIÓN DE ADMINISTRACIÓN DE PERSONAL

C.P. JOSÉ FERNANDO MARTÍNEZ RODRÍGUEZ

c.c.p.- Mtro. Héctor Alberto Arreola Leal.- Director General de Administración del Instituto Nacional de Migración.- Para su conocimiento.
c.c.p.- Lic. Lourdes del Carmen Paredes Abad.- Directora de Normatividad y Control del Instituto Nacional de Migración.- Mismo fin.
c.c.p.- C. Agustín Talavera Muñoz.- Subdirector de Planeación e Ingreso de Personal del Instituto Nacional de Migración.- Mismo fin.

Supervisó: Miguel Ángel Morales Gómez
Revisó: Oscar Zochipa Juárez
Elaboró y verificó: Edgar Eduardo Martínez Escalante

VOLANTE: 10131-DAP

.

Del anterior documento, podemos observar que el INM, contestó que desde el 2012 aún tiene en sus archivos el expediente único de personal, el cual contiene:

- nombre,
- domicilio particular,
- sexo,
- estado civil,
- RFC,
- CURP,
- teléfono particular,
- número de empleado,
- huellas digitales,
- fotografía,
- ciudad de origen,
- edad,
- además, contiene datos de mi nacionalidad,
- estado de salud que tenía al momento de la expedición del documento médico,

finalizando, diciendo que los datos personales son enunciativos más no limitativos.

Asimismo, acepta haber transmitido mis datos personales a la Secretaría de Gobernación, por ser el INM un órgano desconcentrado de ésta última. También se admite haber transmitido mis datos personales a la Plataforma México, fundamentando su actuar en el Acuerdo por el que se reconoce al Instituto Nacional de Migración como instancia de seguridad nacional, publicado en el Diario Oficial de la Federación el 18 de mayo de 2005; así como en lo establecido en los artículos 122 y 123 de la Ley General del Sistema Nacional de Seguridad Pública, publicada en el Diario Oficial de la Federación 2 de enero de 2009, la cual refiere:

> ***Artículo 122.-*** *El Registro Nacional de Personal de Seguridad Pública, conforme lo acuerden las Conferencias Nacionales de Procuración de Justicia y de Secretarios de Seguridad Pública, contendrá la información*

actualizada, relativa a los integrantes de las Instituciones de la Federación, el Distrito Federal, los Estados y los Municipios, el cual contendrá, por lo menos:

I. *Los datos que permitan identificar plenamente y localizar al servidor público, sus huellas digitales, fotografía, escolaridad y antecedentes en el servicio, así como su trayectoria en la seguridad pública;*

II. *Los estímulos, reconocimientos y sanciones a que se haya hecho acreedor el servidor público, y*

III. *Cualquier cambio de adscripción, actividad o rango del servidor público, así como las razones que lo motivaron.*

Cuando a los integrantes de las Instituciones de Seguridad Pública se les dicte cualquier auto de procesamiento, sentencia condenatoria o absolutoria, sanción administrativa o resolución que modifique, confirme o revoque dichos actos, se notificará inmediatamente al Registro.

Artículo 123.- *Las autoridades competentes de la Federación, el Distrito Federal, los Estados y los municipios inscribirán y mantendrán actualizados permanentemente en el Registro los datos relativos a los integrantes de las Instituciones de Seguridad Pública, en los términos de esta Ley.*

Para efectos de esta Ley, se consideran miembros de las Instituciones de Seguridad Pública, a quienes tengan un nombramiento o condición jurídica equivalente, otorgado por autoridad competente.

La infracción a esta disposición se sancionará en términos de la presente Ley.

El INM dentro de la respuesta, menciona que del análisis realizado a mi expediente no se desprende información relativa a haber sido transmitidos datos personales y sensibles, incluidos los datos biométricos a agencias internacionales de seguridad.

De la respuesta a mi solicitud de acceso a la información, pareciera que la transferencia de mis datos se realizó bajo el amparo de la normatividad en ese entonces vigente, sin embargo, si nos remitimos a lo establecido en los artículos anteriormente mencionados no es así.

En los artículos 16 y 18 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, establecen que se deberá observar en el tratamiento los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, y que todo tratamiento de datos personales que efectúe el responsable deberá estar justificado por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera.

Del análisis a dichos artículos, podemos observar que el hecho de que un servidor público de alguna instancia de seguridad nacional como lo es el Instituto Nacional de Migración, en su caso, firme de manera expresa el consentimiento de que sus datos personales serán tratados en el lugar en el cual ingresa a laborar, sin especificar si realizarán alguna transferencia por medios digitales de los mismos, no significa que se haya obtenido la autorización expresa que de los mismos puedan ser tratados en otro lugar distinto, ya que en caso de ser así, el Instituto Nacional de Migración deberá informar, en su caso, los lugares a los que después serán transferidos los datos personales. Toda vez que el titular de los datos tiene el derecho de conocer los lugares a los cuales se destinarán, ya que nunca se obtuvo de éste el consentimiento expreso para realizar un tratamiento distinto de sus datos a la inicialmente informada, y que no se le informe que aún después de no laborar en dicho centro de trabajo, los lugares en los cuales se encuentran sus datos personales, así como la temporalidad y la supresión de los mismos

Es entonces, en donde se encuentra la problemática de análisis de este trabajo de investigación, siendo que al no existir por parte del sujeto obligado el cumplimiento de los principios de finalidad e información, al transferir a otro sujeto obligado los datos de su trabajador sin informar de manera expresa el destino de éstos, no puede considerarse que se encuentran debidamente protegidos los datos, o en su caso que se cumpla el objetivo de la ley de la materia.

Retomando lo establecido por el artículo 18 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, el cual establece que *“todo tratamiento de datos personales que efectúe el responsable deberá estar justificado*

por finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera", esto no se cumple a cabalidad con los servidores públicos del Instituto Nacional de Migración.

Lo anterior, es así ya que como lo hemos venido analizando el consentimiento para el tratamiento de datos personales, se otorga sin tener el conocimiento pleno, por parte del servidor público, del destino variado que tendrán sus datos. No cumpliéndose a cabalidad lo establecido por el citado artículo 18 en cuanto a las finalidades concretas y explícitas, ya que no se señala de manera expresa la finalidad del tratamiento de los datos por parte de los sujetos obligados a las cuales serán enviados los mismos a través de medios digitales por parte del Instituto Nacional de Migración, ni explícitas al no establecer el tratamiento que se les dará en estos lugares.

El mencionado artículo 22 de la LGPDPPSO, no contraviene lo establecido por el artículo 18 de dicha ley, ya que el primero sólo determina cuáles son las causales de excepción de la transferencia de datos sin la manifestación expresa del titular, siendo que el segundo establece la finalidad de los datos.

Es en este tenor, que aún y cuando el servidor público tenga noción o conocimiento indirecto de los destinos en los cuales serán almacenados sus datos personales, no tiene la certeza plena del tratamiento que se les dará a los datos. O en su caso, si en estos lugares, a su vez habrá alguna transferencia a otro ente de gobierno o en su caso a particulares.

Dado lo anterior, la importancia de tener conocimiento del tratamiento que les dará el empleador a los datos personales del titular radica que en caso de que exista algún uso no autorizado de éstos, el titular tenga el conocimiento exacto de donde han sido tratados sus datos personales.

Es por ello, la importancia de informar al titular de los datos personales, en cuanto al tratamiento y almacenamiento de sus datos, tanto en el ámbito de atribuciones del empleador, así como de los otros lugares a los cuales son transferidos los datos a través de medios digitales, en el ejercicio de sus funciones

cuando se trata de instancias de seguridad nacional como lo es el Instituto Nacional de Migración, tal como lo menciona la autora Ana Isabel Hernán Ortiz *"el derecho del individuo a decidir por sí en qué medida o en qué circunstancias desea compartir con terceras personas sus pensamientos, sentimientos y expresiones personales"*.[50]

De lo anteriormente expuesto podemos concluir que el caso del tratamiento de protección de datos personales en las instancias de seguridad nacional en particular el Instituto Nacional de Migración es *sui generis*, toda vez que no informa a las personas que ingresan a laborar la finalidad de los datos, así como del tratamiento que se les dará tanto cuando se encuentren en activo como cuando termine su relación laboral y mucho menos el tiempo que se resguardarán dichos datos al término del trabajo.

De esta manera tenemos que se vulneran los principios de finalidad e información establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como lo establecido en el Convenio 108, del cual México ya es parte, y de lo cual podemos retomar lo que menciona Abel Téllez Aguilera al mencionar que el derecho a la protección de datos es el que *"tiene como objeto garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho afectado"*.[51]

[50] Herrán Ortiz, Ana Isabel, "La violación de la intimidad en la protección de datos personales". Editorial Dykinson, Madrid, 1998, p 2.

[51] Téllez Aguilera, Abel, "Nuevas tecnologías. Intimidad y protección de datos", Madrid: Edisafer, 2001, p. 73.

Capítulo 4.

Transferencia internacional de Datos Personales por medios electrónicos. Modelo de Solución.

Capítulo 4

4.1 Transferencia internacional de Datos Personales por medios electrónicos

Al día de hoy, la interacción social, cultural y económica, hace necesario un intercambio de información más frecuente entre los diferentes países. Conforme ha ido avanzando el desarrollo de las tecnologías de la información, la transferencia de datos vía electrónica es cada vez más común.

Dentro de estos datos, se encuentran los de carácter personal, los cuáles con los recursos de las tecnologías de la información, cada vez hace más fácil su transmisión, sin embargo, por el hecho de ser fácil ésta, no quiere decir que la misma se haga de manera indiscriminada y sin ninguna regulación. Por lo cual, cada país en su búsqueda de protección a los datos personales, se han dado cuenta de la necesidad de regular el tratamiento de los mismo dentro de su territorio, así como cuando éstos son transmitidos a nivel internacional.

En nuestro país los datos personales son información útil para las diferentes instituciones que realizan el tratamiento de éstos en el ámbito de sus atribuciones, ya sea éstas de carácter nacional o internacional. Por lo que al tratarse de instancias de seguridad nacional, el tratamiento de los datos personales se vuelve aún más importante en el desarrollo de sus actividades cotidianas, es por ello, que la transmisión con otras entidades a través de medios electrónicos es cada día más frecuente y necesaria para la consecución de sus objetivos institucionales.

En el caso de México como anteriormente lo hemos revisado, la transmisión de los datos personales entre entes públicos se regula por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la cual en su artículo 6 establece que el Estado garantizará la privacidad con la limitación de la seguridad nacional.

> *Artículo 6. El Estado garantizará la privacidad de los individuos y deberá velar porque terceras personas no incurran en conductas que puedan afectarla arbitrariamente. El derecho a la protección de los datos personales*

solamente se limitará por razones de seguridad nacional, en términos de la ley en la materia, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Como podemos observar, se establece que el derecho a la protección de datos personales dentro de nuestro país será limitado por razones de seguridad nacional.

Sin embargo, la transferencia de datos personales por medios electrónicos con entes internacionales ¿de qué manera es regulado?

En 1980 la Organización para la Cooperación y el Desarrollo Económico (OCDE), emitió las Directrices sobre Protección de Privacidad y flujos transfronterizos de datos personales,[52] donde se da una guía para la recolección y tratamiento de la información personal; las directrices son claras y tienen flexibilidad para su aplicación.

En su definición Segunda, establece que serán aplicables tanto al sector público como al sector privado. Asimismo, estable diversos principios como lo son el de recogida, calidad de los datos, especificación de los fines, limitación de uso, salvaguarda de la seguridad, transparencia, participación individual y principios de responsabilidad (definiciones 7 a 13).

En su definición 17 establece que todo país deberá evitar la reexportación de los datos personales, si el país de destino no respeta dichas directrices.

Por otra parte, los países miembros deberán facilitar el intercambio de información, así como procurar la ayuda mutua en procedimientos de investigación (definición 21).

Como podemos observar, estas disposiciones establecen que pueda existir el intercambio de datos personales, ya sea de manera física o de manera electrónica

[52] Se pueden consultar en http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf (Consultado el 4 de diciembre de 2019)

entre los países miembros, cumpliendo con los principios establecidos en las Directrices.

Asimismo, establece que los datos puedan compartirse por temas de investigación, lo cual es el principio de las labores de inteligencia en los temas de seguridad nacional.

4.2 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

En la Comunidad Europea, se expide el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)[53].

Este Reglamento establece las normas para el tratamiento de los datos personales y a la libre circulación de tales datos, asimismo, tiene aplicación al tratamiento total o parcial automatizado de los datos personales que se encuentren en un fichero (artículos 1 y 2).

De la misma manera, establece los principios a observar en el tratamiento como son la licitud, lealtad, transparencia, fines determinados, explícitos y legítimos, adecuados, pertinentes, limitados, exactos, limitación plazo de conservación, integridad y confidencialidad y responsabilidad proactiva (artículo 5).

Establece el tratamiento en diversas categorías de datos personales, donde se pueden determinar los diversos casos en los cuales algún titular de los datos puede exigir el cumplimiento (artículo 9).

[53] Se pueden consultar en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES (Consultado el 4 de diciembre de 2019)

Asimismo, se establece la información que debe facilitarse cuando los datos personales fueron obtenidos a través del titular de los datos, así como cuando los datos no se obtuvieron a través de éste (artículos 13 y 14).

En este Reglamento se establece el derecho de rectificación; el derecho a la supresión o como comúnmente se conoce el derecho al olvido; el derecho a la limitación del tratamiento; derecho de portabilidad de datos, así como el derecho a oposición (artículos 16, 17, 18, 20 y 21).

Dentro del Reglamento hace la aparición el Delegado de Protección de Datos, quien entre otras funciones supervisará el cumplimiento del ordenamiento legal en comento de la Unión Europea o de los Estados miembros (artículo 39).

4.3 Transferencia internacional vía electrónica de datos personales de los servidores públicos en instancias de seguridad nacional.

Como hemos explicado con anterioridad, en nuestro país los servidores públicos que laboran en instancias de seguridad nacional, por el simple hecho de trabajar en dichas instancias están expuestos a que sus datos personales sean transmitidos vía electrónica con algún otro país que tenga cooperación internacional en materia de seguridad pública, argumentando temas de seguridad nacional.

Esto es así, toda vez que, al momento de depositar sus datos en la Plataforma México, pueden acceder a ésta diversos organismos de otros países los cuales de manera automatizada pueden realizar diversas consultas del servidor público en cuestión.

Esta plataforma contiene en sus bases de datos, entre otros los datos personales de los servidores públicos que laboran en instancias de seguridad nacional en los tres niveles de gobierno (federal, estatal y municipal), con la finalidad de que sean identificables ante cualquier instancia de seguridad nacional.

De lo anterior, tenemos que, por el simple hecho de laborar en una instancia de seguridad nacional, el servidor público deberá estar expuesto a que sus datos sean tratados de manera automatizada en un país externo, lo cual lo deja en estado de vulnerabilidad, toda vez que dicha situación no fue hecha de su conocimiento a

través de los avisos de privacidad que en su momento el lugar de trabajo le debió haber hecho de su conocimiento.

Aunado a lo anterior, tenemos que los datos personales por sí mismos son información muy valiosa, sin embargo, no solo es el tratamiento automatizado que se les dará, sino que el medio de transmisión que es a través del internet hace que al transmitir la información exista un alto riesgo de que algún externo pueda conocer dicha información.

Es por ello, que el intercambio de información de manera transfronteriza requiere tener óptimos controles de seguridad, tanto a nivel jurídico como a nivel de infraestructura, es por eso que el país que realice el tratamiento automatizado de los datos personales, deberá protegerlos contra riesgos y accesos no autorizados.

En este tenor, tenemos que si bien es cierto la transmisión de datos vía electrónica a nivel internacional está permitida, también lo es que al titular de los datos, como el caso que nos ocupa el servidor público de la instancia de seguridad nacional deberá ser informado de tales transmisiones, sobre todo porque éste tiene derecho a conocer la manera en cómo serán tratados sus datos, aunado a que debe de conocer de manera precisa la seguridad informática con la cual estarán resguardados sus datos desde el momento de la recolección de los mismos, el camino hacia su destino y el resguardo final.

De esta manera, tenemos que en nuestro país los avisos de privacidad que se dan a conocer a las personas, en particular a los servidores públicos que laboran en instancias de seguridad nacional, únicamente se limitan a establecer los datos generales del destino de los datos.

4.4 Modelo de Solución estratégica

Una vez expuesto todo lo anterior, es evidente que, al ingresar al servicio público dentro de una instancia de seguridad nacional, los datos personales del servidor público al ser compartidos de manera oficial a través de medios digitales quedan en estado de vulnerabilidad, toda vez que su tratamiento no cumple con los principios de finalidad y tratamiento. Primero por no cumplir con el principio de información al

no existir notificación expresa al titular de los datos del lugar en donde serán tratados éstos y mucho menos conocer el tiempo de resguardo o de destrucción, en su caso.

Es por ello, que en el caso particular del INM, al ingresar una persona dentro de la estructura de la institución, se le deberá informar de forma explícita y concreta no sólo el tratamiento de datos personales dentro de la institución, sino que los mismos serán transferidos a otros órganos ya sea nacionales o internacionales a través de medios digitales.

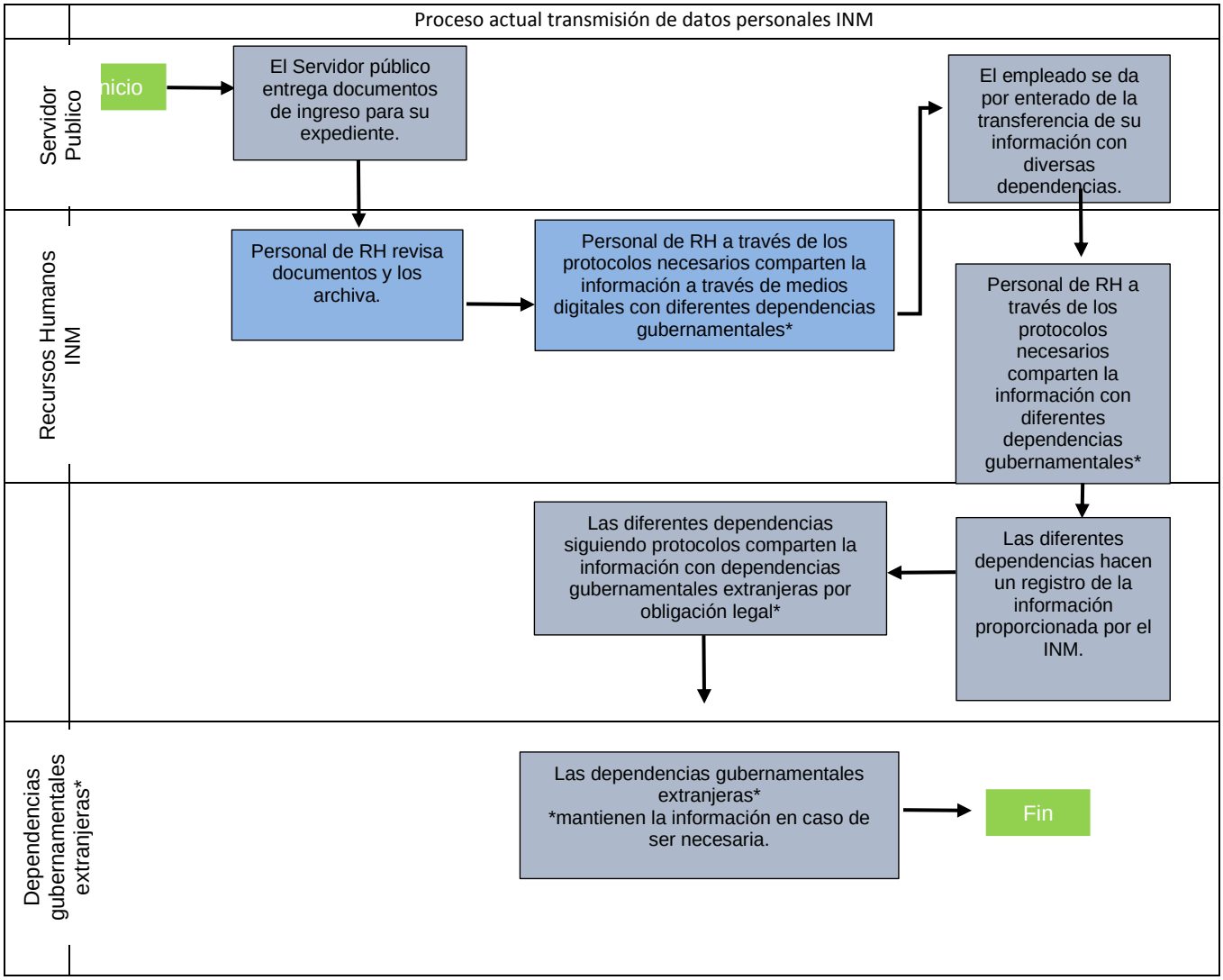
La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en su artículo 22 establece que la transferencia entre sujetos obligados no requerirá de la autorización expresa del titular de los datos, siempre y cuando se realice para los fines solicitados, y que sea parte de sus atribuciones el recolectar dicha información.

En este caso, el artículo 80 de la Ley antes citada, si bien hace referencia a que cuando la transferencia sea por razones de seguridad nacional, no se requiere el consentimiento del titular de los datos, sin embargo, como hemos visto en el presente trabajo, el hecho que no se requiera del consentimiento del servidor público para la transferencia de sus datos personales a otro sujeto obligado a través de medios digitales, no quiere decir que no se deba notificar de manera expresa los lugares a los cuales van a ser transferidos los datos aún tratándose de instancias de seguridad nacional.

Esto es así, una vez que el Instituto Nacional de Migración obtenga los datos personales del trabajador, deberá notificar de manera expresa, esto aún y cuando no existe una obligación legal de realizarla, al titular de los datos a efecto de que éste conozca de manera precisa los lugares a los cuales serán transferidos los datos.

Lo anterior, para que el titular de los datos personales pueda conocer con exactitud los lugares a los cuales serán transferidos dichos datos y que en caso de que querer ejercer alguna acción legal, ya sea para hacer uso de los derechos

ARCO, así como en caso de una mala utilización de los mismos, pueda tener la información exacta de las instituciones gubernamentales que realizarán el tratamiento de los datos personales en medios electrónicos.



Fuente: Elaboración Propia

*Dependencias como Secretaria de Seguridad pública, CISEN, Secretaria de Hacienda y Crédito Público, IMSS, Infonavit y Secretaria de Función pública

1 Proceso actual de transmisión internacional de datos personales

Lo anterior, con el objeto de que el servidor público tenga conocimiento certero y oportuno del tratamiento de sus datos personales.

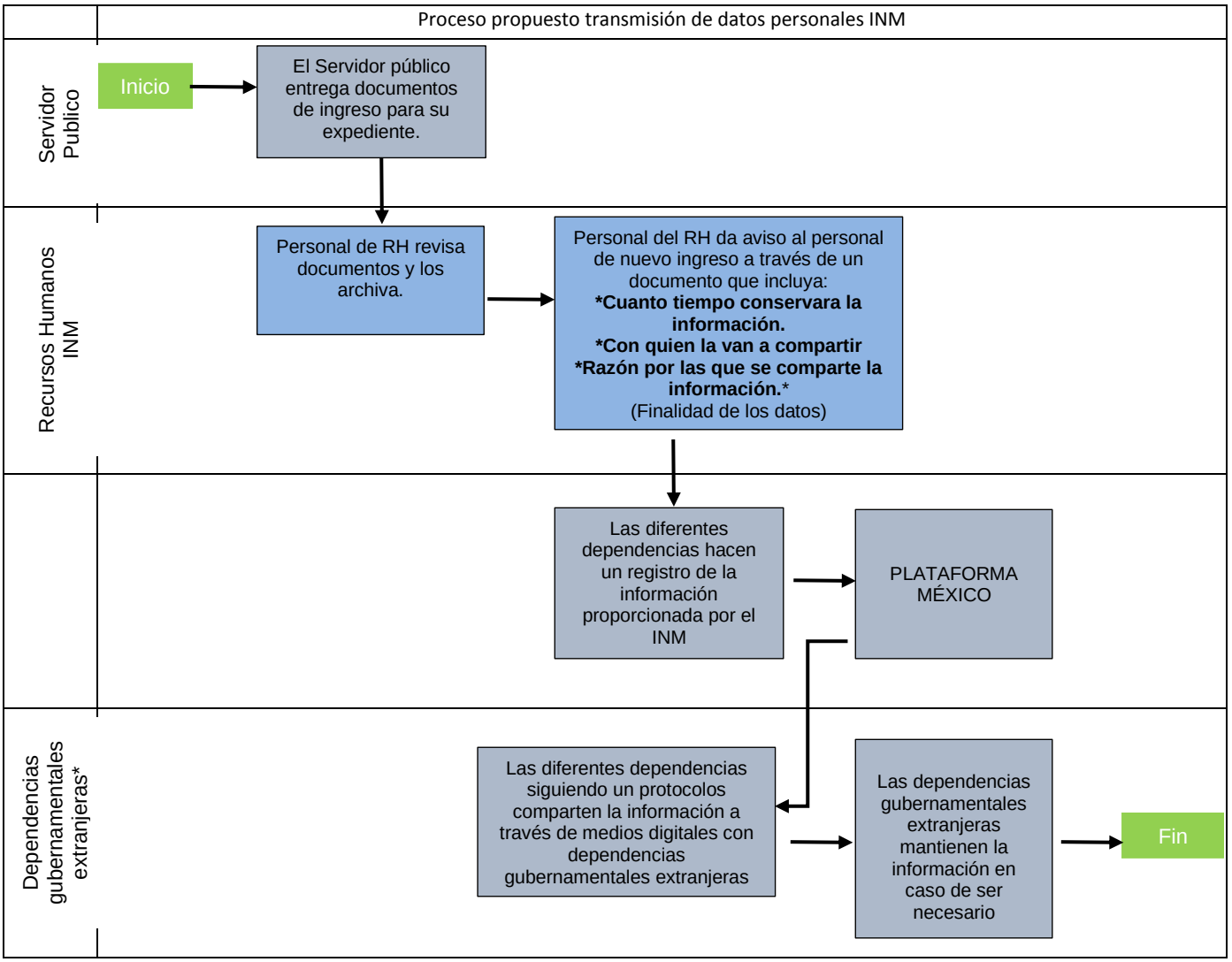
4.4.1 Metodología a emplear

La metodología que se propone es a través de la estrategia para resolver la problemática planteada, es que en el caso particular del Instituto Nacional de Migración, en el momento de ingreso del servidor público, independientemente de que se cumpla con el aviso de privacidad el cual retomando lo establecido por el artículo 27 de la Ley General de protección de Datos Personales en Posesión de Sujetos Obligados informa el tratamiento de sus datos personales y sensibles dentro de la institución, de manera expresa y que dicha notificación forme parte del expediente laboral del servidor público, así como el acceso a los derechos ARCO, debe manifestarse de manera expresa por parte de la institución el destino de cada uno de sus datos y los lugares a los cuales se enviarán sus datos a través de medios digitales, así como el tiempo de resguardo y destrucción de los mismos, conforme a lo establecido en el Convenio 108 para la Protección de las Personas con respecto al tratamiento automatizado de los datos de carácter personal. (Artículo 8)

Esto es, que una vez que el titular de los datos tenga conocimiento del aviso de privacidad, se deberá especificar cada uno de los lugares a los cuales serán realizadas transferencias nacionales o internacionales de sus datos de manera legal. Es decir, de acuerdo a lo establecido en el artículo 70, fracción II de la Ley General de Protección de Datos en Posesión de Sujetos Obligados, las transferencias de datos que realice el INM a otro sujeto a través de medios digitales.

Derivado de lo anterior, se establecerá por ejemplo si los datos personales son transferidos a la Secretaría de Gobernación, a la Secretaría de Hacienda y Crédito Público, al ISSSTE, al FOVISSSTE, se deberá especificar el tipo de datos a enviar por medios digitales, si sólo se trata de datos personales, datos sensibles o de alguna otra naturaleza, el área en específico a la cual se mandarán, el responsable de los datos en esa institución, el tratamiento que se les dará, si los mismos formarán parte de un padrón o registro público, la fecha de envío y el medio por el cual se envían, así como el tiempo en que se encontrarán resguardados y posteriormente suprimidos (artículo. 23).

En caso de enviarse datos adicionales, complementarios o actualizaciones se deberá notificar al titular de los datos de dicha acción. Esto a efecto de que el servidor público siga informado del destino de los datos, siempre y cuando dicha notificación sea realizada bajo la premisa que será al menor costo posible, utilizando los medios electrónicos para optimizar recursos.



Fuente: Elaboración propia

*Dependencias como Secretaria de Seguridad pública, CISEN, Secretaria de Hacienda y Crédito Público, IMSS, Infonavit y Secretaria de Función pública

2 Proceso propuesto para informar de la transmisión de datos personales

En este modelo de solución, lo que se busca es que el INM notifique al servidor público de cada una de las transmisiones de datos personales, especificando el lugar al cual se compartieron dichos datos. Una vez que se especifique el lugar al cual se transmitieron, se deberá informar de cuál será el tratamiento de éstos, la finalidad y la temporalidad, para que en el caso de que no se ocupen los mismos, se establezca un periodo de destrucción de los mismos.

4.4.2 Diseño de estrategias

En este ejemplo, podemos observar que, al ser el Instituto Nacional de Migración, el sujeto obligado que obtiene, organiza y conserva la información, actúa como el que transfiere a otro sujeto obligado por medios digitales. Ésta deberá notificarse al titular de los datos personales. Así tendrá la certeza del tratamiento de los datos. Lo cual como hemos comentado servirá de base para que al tener conocimiento de los lugares en los cuales son tratados los datos en caso de exista algún mal uso de los datos personales, pueda identificar de manera más precisa el lugar en donde se realizó este tratamiento ilícito.

Propuesta

Dicha acción de notificación de transferencia de datos personales al titular de los mismos, en materia de seguridad nacional se realizará de la siguiente manera:

1.- En primer lugar, el proceso de reclutamiento y alta del servidor público deberá ser modificado a efecto de agregar la notificación de destino de datos personales.

2.- Asimismo, se deberá ingresar dicha notificación con la firma del servidor público dentro de su expediente en el INM.

3.- En caso de mal uso de los datos personales del titular, podrá identificar si, en su caso, el sujeto obligado presumiblemente incumplió con algunas de sus obligaciones y si derivado de este incumplimiento existiere algún daño hacia su persona.

4.- Derivado de lo anterior, el titular de los datos personales determinará la acción legal que emprenderá atendiendo a la acción contraria a derecho, realizando las denuncias respectivas.

Conclusiones

El objetivo general del presente trabajo de investigación es proponer un modelo de solución estratégica para una adecuada transferencia de datos personales de los servidores públicos que laboren en instancias de seguridad nacional, como es el Instituto Nacional de Migración., que se adapte a la regulación en la materia y con ello dicho personal tenga la facultad de ejercer sus derechos ARCO, ya que siendo parte del servicio público y que dicho tratamiento de datos se da inclusive cuando el servidor público ya se encuentra fuera del servicio, a través de medios físicos o medios digitales, en posesión de sujetos obligados, lo cual puede llegar a menoscabar su derecho de Protección de Datos Personales al desconocer las instancias a las cuales son transmitidos, su temporalidad, finalidad concreta y eliminación, para que los titulares de los datos, en su caso, una vez conocidos todos los lugares en los cuales han sido tratados sus datos personales.

De lo anterior, recapitularemos lo abordado en los diversos capítulos:

1. Capítulo 1. La protección de datos personales es un tema que ha ido evolucionando a través de los años en los diversos países a través de la normativa tanto de carácter internacional, así como en lo particular sobre todo en los países Europeos, los cuales han establecido de manera clara y precisa las reglas de su tratamiento.

En dichos países se han establecido los límites de la actuación del Estado en cuanto a la privacidad de las personas, lo cual repercute que las personas se encuentren protegidas por la normatividad en caso del mal uso de los datos personales.

En este tenor, México no ha quedado exceptuado de dicha evolución y ha emitido diversa normatividad en materia de protección de datos personales, las cuales han establecido la precisión de datos personales, las instituciones que vigilarán su protección, así como la manera en que serán tratados los mismos.

2. Capítulo 2. México a partir del año 2002, ha promulgado diversas normatividades en las cuales se ha buscado la protección de los datos personales, así como el tratamiento de éstos.

Cabe destacar, que se inició con la protección únicamente del poder Ejecutivo y hoy en día se encuentran obligados a brindar dicha protección a los tres poderes de la unión, los órganos autónomos, los sindicatos, los partidos políticos, e inclusive los particulares, con lo cual podemos observar la evolución a través de los años en la visión de proteger los datos personales.

Sin embargo, el tema de protección de los datos personales de los servidores públicos que laboran en instancias de seguridad nacional, no es del todo claro, por lo cual se realizará un análisis de esta figura en nuestro país.

3. Capítulo 3. El caso del tratamiento de protección de datos personales en las instancias de seguridad nacional en particular el Instituto Nacional de Migración es *sui generis*, toda vez que no son informados los servidores públicos la finalidad de los datos, así como del tratamiento que se les dará tanto cuando se encuentren en activo como cuando termine su relación laboral, tampoco se informa la temporalidad en que se resguardarán los datos personales.
4. Capítulo 4. En este tenor, tenemos que si bien es cierto la transmisión de datos vía electrónica a nivel internacional está permitida, también lo es que al titular de los datos, como el caso que nos ocupa el servidor público de la instancia de seguridad nacional deberá ser informado de tales transmisiones, sobre todo porque éste tiene derecho a conocer la manera en cómo serán tratados sus datos, aunado a que debe de conocer de manera precisa la seguridad informática con la cual estarán resguardados sus datos desde el momento de la recolección de los mismos, el camino hacia su destino y el resguardo final.

De esta manera tenemos que se vulneran los principios de finalidad e información establecidos en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, así como lo establecido en el Convenio 108, del cual México ya es parte.

5. Una vez desarrollado el presente trabajo, concluimos que si bien es cierto en México se encuentra regulada la materia de protección de datos, mediante diversas legislaciones y que a través de éstas se regulan el tratamiento y las transferencias de los datos personales que se encuentran en posesión de Sujetos Obligados. También lo es, que el caso de los servidores públicos que laboran en instancias de seguridad nacional como lo es el Instituto Nacional de Migración, al ser un caso *sui generis*, no se encuentra del todo regulado.

De lo anterior, tenemos que se cumplió con el objetivo del presente trabajo de investigación, al haber quedado demostrado que, en el procedimiento de tratamiento de datos personales del Instituto Nacional de Migración, no se cumple con. La protección de datos de la cual debe gozar cualquier persona, en caso particular, cualquier servidor público.

Es por ello, que como solución se propone que es necesario informar a los servidores públicos que laboran en la instancia de seguridad nacional Instituto Nacional de Migración la finalidad del tratamiento de sus datos personales de manera precisa, para lo cual es necesario, modificar su procedimiento actual, e incorporar dentro de sus avisos de privacidad la especifidad de la manera en que serán tratados sus datos, informando a los lugares a los cuales serán transmitidos y la manera en que serán resguardados, con el objetivo de que el servidor público tenga conocimiento pleno de ello.

Bibliografía

BASTERRA, Marcela I, México 2008: *"Protección de Datos Personales"*, Ediar EDRS

GARRIDO IGLESIAS, Romina, 2015: *"La seguridad en el tratamiento de datos personales"*, en Reyes Olmedo, Patricia (coord.), *Ciudadanas 2020 III*, Chile, 2015

GÓMEZ ROBLEDO, Alfonso; Ornelas Núñez, Lina, 2003: *"Protección de Datos Personales en México. El caso de Poder Ejecutivo en México"*, UNAM Instituto de investigaciones jurídicas, México.

HASSEMER, Winfried. 1997: *El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales*. Bueno Aires: Editores del Puerto.

HERRÁN ORTÍZ, Ana Isabel, 1998: *"La violación de la intimidad en la protección de datos personales"*, Madrid, Editorial Dykinson,

MADRID CONESA, Fulgencio, 1984: "*Derecho a la intimidad, informática y Estado de derecho"*, Valencia, Universidad de Valencia.

MEJÁN, Luis Manuel C. 1994: *"El Derecho a la Intimidad y la Informática"*, México, Porrúa.

ORNELAS NÚÑEZ, Lina, 2012: *"Curso Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento"*, Tirant Lo Blanch Formación. México.

Legislación:

Ley General de Protección de Datos Personales de Sujetos Obligados, 2017, México.

Ley General de Transparencia y Acceso a la Información Pública, 2015, México.

Ley de Seguridad Nacional, 2005, México.

Páginas web

Agencia Estatal Boletín Oficial del Estado. en https://www.boe.es/boe/dias/2001/01/04/pdfs/T00104-00118.pdf

(consultada el 27 de julio de 2018).

BOE Legislación Consolidada, en https://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf

(consultada el 18 de diciembre de 2018)

Congreso de los Diputados España. Constitución Española de 1978, en

http://www.congreso.es/docu/constituciones/1978/1978_cd.pdf

(Consultada el 18 de septiembre de 2018)

EUR-Les Access to European Union law, Protección de los datos personales. Directiva 95/46/CE, en http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM%3Al14012

(consultada el 27 de julio de 2018).

DºChile Entre tecnología y humanidad, Sentencia de 15 de diciembre de 1983, del Tribunal Constitucional Federal Alemán, Ley del Censo, en http://www.derecho-chile.cl/sentencia-de-15-de-diciembre-de-1983-del-tribunal-constitucional-federal-aleman-ley-del-censo/(consultada el 25 de julio de 2019)

Diario Oficial de las Comunidades Europeas, en http://www.europarl.europa.eu/charter/pdf/text_es.pdf (consultada el 2O de septiembre de 2018).

Diario Oficial de la Federación, en http://dof.gob.mx/nota_detalle.php?codigo=5092143&fecha=01/06/2009

(consultada el 21 de septiembre de 2018).

Diario Oficial de la Federación, en http://www.dof.gob.mx/nota_detalle.php?codigo=5332003&fecha=07/02/2014

(consultada el 22 de septiembre de 2018)

Diario Oficial de la Federación, Acuerdo 02/2007 del Secretario de Seguridad Pública, por el que se crean el Consejo Asesor y el Comité Técnico de la Plataforma México. 29 marzo de 2007. en: http://www.dof.gob.mx/nota_detalle.php?codigo=4966851&fecha=29/03/2007

Library of Congress. "*The German Federal Data Protection Act has separate provisions for data processing in the public and private sectors."* USA.GOV https://www.loc.gov/law/help/online-privacy-law/2012/germany.php

(consultada el 18 de septiembre de 2018).

Naciones Unidas. Declaración Universal de Derechos Humanos. http://www.un.org/es/universal-declaration-human-rights/ (Consultada el 25 de enero de 2018)

Naciones Unidas. Pacto Internacional de Derechos Civiles y Políticos. https://www.ohchr.org/sp/professionalinterest/pages/ccpr.aspx (Consultada el 25 de enero de 2018)

Revista Chilena de Derecho Informático Autodeterminación informativa y leyes sobre protección de datos, 3. Las leyes de Protección de Datos, en http://web.uchile.cl/vignette/derechoinformatico/CDA/der_informatico_simple/0,1493,SCID%253D14338%2526ISID%253D507%2526PRT%253D14331,00.html

(consultada el 5 de julio de 2018).

Richmond University, en http://confinder.richmond.edu/admin/docs/portugalsp.pdf

(consultada el 18 de septiembre de 2018).

The United States Department of Justice Privacy Act of 1974, en https://www.justice.gov/opcl/privacy-act-1974

https://www.justice.gov/opcl/file/844481/download (consultada el 6 de julio de 2018)

Quiroga Lavié, *Humberto*. , 1995: "*Derecho a la intimidad y objeción de conciencia"*. Bogotá: Universidad Externado de Colombia.

Rosales Ortiz, Mariano Carlos, 2016: "*Prontuario de protección de datos personales"*, México.

Téllez Aguilera, Abel. 2001: "*Nuevas tecnologías. Intimidad y protección de datos"*, Madrid: Edisafer.

Villanueva Ernesto, Nucci Hilda, 2012*: "Comentarios a la Ley Federal de Protección de datos Personales en Posesión de Particulares",* Novum, México.

Tesis

Registro No. 2001108

Localización:

Décima Época

Instancia: Suprema Corte de Justicia (Pleno)

Fuente: *Semanario Judicial de la Federación y su Gaceta,* X, Julio de 2012

Página 243

Tesis: P./J. 12/2012

Jurisprudencia

Materia: Constitucional