# LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS, COMENTADA

inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

**María Solange Maqueo**
Coordinadora Editorial

# LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS, COMENTADA

inai
Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

# DIRECTORIO

**FRANCISCO JAVIER ACUÑA LLAMAS**
COMISIONADO PRESIDENTE

**CARLOS ALBERTO BONNIN ERALES**
COMISIONADO

**OSCAR MAURICIO GUERRA FORD**
COMISIONADO

**BLANCA LILIA IBARRA CADENA**
COMISIONADA

**MARÍA PATRICIA KURCZYN VILLALOBOS**
COMISIONADA

**ROSENDOEVGUENI MONTERREY CHEPOV**
COMISIONADO

**JOEL SALAS SUÁREZ**
COMISIONADO

# COMITÉ EDITORIAL

**OSCAR M. GUERRA FORD**
PRESIDENTE
**BLANCA LILIA IBARRA CADENA**
**JOEL SALAS SUÁREZ**
**JESÚS RODRÍGUEZ ZEPEDA**
**JOSÉ ROLDÁN XOPA**
**JAVIER SOLÓRZANO ZINSER**
**GERARDO VILLADELÁNGEL VIÑAS**

**CRISTÓBAL ROBLES LÓPEZ**
SECRETARIO TÉCNICO

Derechos Reservados D.R.

**Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales** (INAI).

Insurgentes Sur 3211, colonia Insurgentes Cuicuilco,
Alcaldía de Coyoacán, Ciudad de México, C.P. 04530.

Primera edición, noviembre de 2018.

Impreso en México, *Printed in Mexico.*
Ejemplar de distribución gratuita.

# ÍNDICE

**PRESENTACIÓN** María Solange Maqueo ..... 9

**PRÓLOGO** Carlos Alberto Mata Prates ..... 15

**SEMBLANZAS DE LOS AUTORES** ..... 21

**REFERENCIA DE SIGLAS Y ACRÓNIMOS** ..... 29

**TÍTULO PRIMERO**
**DISPOSICIONES GENERALES** ..... 31

**Capítulo I**
**Del Objeto de la Ley** ..... 33

*Comentado por María Solange Maqueo* ..... 40

**Capítulo II**
**Del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales** ..... 53

*Comentado por José Antonio Caballero Juárez* ..... 56

**TÍTULO SEGUNDO**
**PRINCIPIOS Y DEBERES** ..... 65

**Capítulo I**
**De los Principios** ..... 67

*Comentado por Nelson Remolina Angarita* ..... 72

**Capítulo II**
**De los Deberes** ..... 91

*Comentado por Andrés Velázquez* ..... 94

**TÍTULO TERCERO**
**DERECHOS DE LOS TITULARES Y SU EJERCICIO** ..... 115

**Capítulo I**
**De los Derechos de Acceso, Rectificación, Cancelación y Oposición** ..... 117

*Comentado por Paulina del Pilar Gutiérrez* ..... 118

**Capítulo II**
**Del Ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición** ..... 137

*Comentado por Miguel Recio Gayo* ..... 141

**Capítulo III**
**De la Portabilidad de los Datos** ..... 157

*Comentado por Oscar R. Puccinelli* ..... 157

**TÍTULO CUARTO**
**RELACIÓN DEL RESPONSABLE Y ENCARGADO** ..... 185

**Capítulo Único**
**Responsable y Encargado** ..... 187

*Comentado por Miguel Recio Gayo* ..... 190

**TÍTULO QUINTO**
**COMUNICACIONES DE DATOS PERSONALES** ..... 205

**Capítulo Único**
**De las Transferencias y Remisiones de Datos Personales** ..... 207

*Comentado por María Mercedes Albornoz* ..... 209

**TÍTULO SEXTO**
**ACCIONES PREVENTIVAS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES** ..... 221

**Capítulo I**
**De las Mejores Prácticas** ..... 223

*Comentado por José Luis Piñar Mañas* ..... 225

**Capítulo II**
**De las Bases de Datos en Posesión de Instancias de Seguridad, Procuración y Administración de Justicia** ..... 239

*Comentado por Mónica Estrada Tanck* ..... 240

**TÍTULO SÉPTIMO**
**RESPONSABLES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS SUJETOS OBLIGADOS** ..... 263

**Capítulo I**
**Comité de Transparencia** ..... 265

*Comentado por Jimena Moreno González* ..... 266

**Capítulo II**
**De la Unidad de Transparencia** ..... 273

*Comentado por Jimena Moreno González* ..... 274

**TÍTULO OCTAVO**
**ORGANISMOS GARANTES** ..... 279

**Capítulo I**
**Del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales** ..... 281

*Comentado por Jimena Moreno González* ..... 284

**Capítulo II**
**De los Organismos Garantes** ..... 291

*Comentado por Gisela María Pérez Fuentes* ..... 293

**Capítulo III**
**De la Coordinación y Promoción del Derecho a la Protección de Datos Personales** ..... 305

*Comentado por Gisela María Pérez Fuentes* ..... 306

**TÍTULO NOVENO**
**DE LOS PROCEDIMIENTOS DE IMPUGNACIÓN EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS** ..... 317

**Capítulo I**
**Disposiciones Comunes a los Recursos de Revisión y Recursos de Inconformidad** ..... 319

*Comentado por Ana Elena Fierro* ..... 322

**Capítulo II**
**Del Recurso de Revisión ante el Instituto y los Organismos Garantes** ..... 335

*Comentado por Ana Elena Fierro* ..... 341

**Capítulo III**
**Del Recurso de Inconformidad ante el Instituto** ..... 349

*Comentado por Alessandra Barzizza y Mauricio Castillo* ..... 353

**Capítulo IV**
**De la Atracción de los Recursos de Revisión** ..... 363

*Comentado por María Solange Maqueo* ..... 365

**Capítulo V**
**Del Recurso de Revisión en Materia de Seguridad Nacional** ..... 375

*Comentado por Michael G. Núñez Torres y Alonso Cavazos Guajardo* ..... 376

**Capítulo VI**
**De los Criterios de Interpretación** ..... 389

*Comentado por Olivia Andrea Mendoza* ..... 389

**TÍTULO DÉCIMO**
**FACULTAD DE VERIFICACIÓN DEL INSTITUTO Y LOS ORGANISMOS GARANTES** ..... 397

**Capítulo Único**
**Del Procedimiento de Verificación** ..... 399

*Comentado por Alessandra Barzizza y Mauricio Castillo* ..... 401

**TÍTULO DÉCIMO PRIMERO**
**MEDIDAS DE APREMIO Y RESPONSABILIDADES** ..... 413

**Capítulo I**
**De las Medidas de Apremio** ..... 415

*Comentado por Olivia Andrea Mendoza* ..... 417

**Capítulo II**
**De las Sanciones** ..... 425

*Comentado por Olivia Andrea Mendoza* ..... 428

**TRANSITORIOS** ..... 435

*Comentados por María Solange Maqueo* ..... 436

# PRESENTACIÓN

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados es producto de la experiencia acumulada en nuestro país por casi tres lustros. Para apreciar su relevancia y advertir los cambios que supone en la propia forma de entender y aplicar el derecho a la protección de datos personales es conveniente realizar, aunque sea brevemente, una mirada en retrospectiva de su desarrollo normativo.

Al respecto, cabe señalar que la incorporación del derecho a la protección de datos personales en México se produce en un contexto muy particular, distinto del desarrollo que tuvo, por ejemplo, en el contexto internacional, en los Estados miembros de la Unión Europea o en algunos países latinoamericanos, como Argentina, Uruguay o Colombia, por citar unos cuantos, que han adoptado una legislación especial en la materia. Esta diferenciación se explica a partir de su recepción en nuestro sistema jurídico bajo el paraguas del derecho de acceso a la información pública y cuya aplicación estaba exclusivamente referida al sector público.

El derecho a la protección de datos personales se introduce por primera vez en México a través de la ahora abrogada Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental de 2002 (LFTAIPG) que establecía dentro de sus objetivos el de “Garantizar la protección de datos personales en posesión de sujetos obligados” (artículo 3, fracción III), así como un desarrollo incipiente de los principios, derechos y deberes que lo conforman. Todo lo cual contaría con una mayor precisión de conceptos a través de los Lineamientos de Protección de Datos Personales emitidos por el Instituto Federal de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (IFAI, ahora INAI) en 2005, pero acotados al propio alcance de la citada ley. En ese sentido, el derecho a la protección de datos personales sería inicialmente un límite o excepción del derecho de acceso a la información, cuyo campo de aplicación cobraría mayor fuerza, más como un criterio de clasificación de la información que como un derecho subjetivo propio a favor de la dignidad humana y la autodeterminación informativa.

La reforma de 2007 al artículo 6º de la Constitución Política de los Estados Unidos Mexicanos mantiene la lógica inicialmente impresa al derecho a la protección de datos personales por la citada LFTAIPG. Seguía prevaleciendo

su categorización como mera excepción del derecho de acceso a la información pública y donde el énfasis estaba puesto en los criterios de clasificación de la información. De tal forma que, a excepción de escasas entidades federativas que adoptaron una legislación especial en la materia y que, incluso, en algunos casos, llegaron a extender los alcances del derecho hacia el sector privado, el derecho a la protección de datos personales permanecía bajo la sombra de los reflectores propios de la transparencia y el acceso a la información.

No obstante, la reforma constitucional de 2007, como se puede observar en el dictamen emitido por las Comisiones Unidas de Puntos Constitucionales y de la Función Pública de la Cámara de Diputados durante el proceso de la misma, supuso el reconocimiento de la estrecha relación entre el derecho a la vida privada y la protección de datos personales sin que ambos llegaran a confundirse. Esto, sin duda alguna, representó un importante avance en el reconocimiento del derecho a la protección de datos personales diferenciado de otros derechos, concretamente del derecho humano a la vida privada, a la intimidad, el honor y la propia imagen. Además, mediante esta reforma constitucional se estableció el principio de reserva de ley para el desarrollo de sus términos y excepciones.

No es sino hasta la reforma constitucional de 2009 a los artículos 16 y 73, fracción XXIX-O que se produce un verdadero cambio de paradigma que dota al derecho a la protección de datos personales de un contenido propio e independiente del derecho de acceso a la información pública. Mediante esta reforma constitucional se extiende, en todo el territorio nacional, el ámbito de protección de las personas por lo que se refiere a sus datos personales mediante la incorporación de los particulares como responsables de su tratamiento. Para esos efectos, la reforma constitucional le confiere al Congreso de la Unión la facultad para legislar de manera exclusiva en la materia. Asimismo, se reconocen los derechos de acceso, rectificación, cancelación y oposición (también conocidos por su acrónimo como derechos ARCO) que hacen explícito el ámbito de autodeterminación informativa del derecho a la protección de datos personales. Entonces, podríamos decir que es precisamente a partir de esta reforma constitucional que el derecho a la protección de datos personales, reconocido en nuestro país, se logra vincular de manera más directa con las preocupaciones que impulsaron su desarrollo en el contexto internacional, donde los riesgos para la privacidad que supone el avance tecnológico y el sentido económico de los datos personales cobran mayor fuerza como argumentos para justificar su propia existencia.

Así, el derecho a la protección de datos personales fue adquiriendo un sentido diverso y expansivo al previsto en su contenido original. A las dificultades de generar criterios de clasificación de la información, evitar un uso indebido y

resguardar debidamente la información personal por parte de las autoridades gubernamentales, se sumaron otras preocupaciones que la incorporación del sector privado como responsable del tratamiento de datos personales hizo más evidentes, tales como la implementación de garantías que permitan la continuidad de la protección de datos personales en los flujos transfronterizos de datos personales, el cómputo en la nube, el rol de los titulares de datos personales como piezas clave para la efectividad del derecho, entre otros aspectos. Todo lo cual se vería reflejado en la Ley Federal de Protección de Datos Personales en Posesión de Particulares de 2010 y, posteriormente, en su Reglamento de 2011, con una clara influencia de los estándares adoptados por la Unión Europea, fundamentalmente a través de la Directiva 95/46/CE del Parlamento Europeo y del Consejo del 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 éstos.

Con ello, las asimetrías entre los distintos regímenes de protección de datos personales —uno aplicable para el sector privado y otro, con las variantes propias del federalismo y la división de poderes, para el sector público— se hicieron patentes. En el ámbito federal, por ejemplo, seguía vigente la LFTAIPG de 2002, cuyo contenido en materia de protección de datos personales contrastaba, por una parte, con las salvaguardas adoptadas por la Ley Federal de Protección de Datos Personales en Posesión de Particulares y por la otra, respecto de otros ordenamientos jurídicos emitidos en el ámbito estatal que, incluso, en algunos casos, contaban con una legislación específica en la materia con un nivel de protección mayor al previsto en el ámbito federal para el sector público.

En ese contexto se produce la reforma constitucional en materia de transparencia, publicada en el *Diario Oficial de la Federación* el 7 de febrero de 2014, misma que obedeció, entre otras cuestiones, a la necesidad de establecer estándares homogéneos en la protección de datos personales en toda la República Mexicana, dadas las acusadas diferencias que se presentaban en los distintos órdenes de gobierno y entre los propios responsables del tratamiento de datos personales. Con este objetivo, la citada reforma constitucional introdujo una profunda transformación, tanto en el diseño institucional de los propios órganos garantes (que los dota de autonomía constitucional a fin de incorporar en un mismo esquema de control y supervisión a los sujetos obligados que no formaran parte de la Administración Pública), como en el desarrollo normativo del derecho (por medio de un cambio en el régimen de facultades y en la profundización del contenido del derecho y de los mecanismos para dotarlo de efectividad).

Precisamente la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados constituye la materialización de la reforma constitucional de 2014. Por medio de ésta se desarrollan los principios, bases y procedimientos establecidos por nuestra carta magna por lo que se refiere al derecho a la protección de datos personales en posesión de los sujetos obligados. Se trata del marco jurídico general aplicable de manera directa a la Federación y a partir del cual los estados adoptan su propio régimen legal y se emiten las diversas medidas regulatorias en los distintos órdenes de gobierno. Dada su reciente creación, se constituye en un ordenamiento jurídico de vanguardia en la región con una clara influencia de los elevados estándares de protección adoptados por la Unión Europea que fortalece los cimientos mismos de su construcción e incorpora importantes novedades que vigorizan el legítimo y debido tratamiento de los datos personales y el ámbito de autodeterminación informativa de las personas.

En ese sentido, la ley general en comento requiere de un análisis y reflexión que coadyuve a facilitar su comprensión entre los servidores públicos, la academia y la sociedad en general. Con ese ánimo, el texto que aquí se presenta constituye el esfuerzo y colaboración de destacados especialistas, tanto nacionales como internacionales, fundamentalmente en materia de protección de datos personales, pero también en otras áreas directamente relacionadas con su aplicación e interpretación, como son el uso de las tecnologías de la información y la comunicación, los derechos digitales y los procedimientos administrativos que permiten su efectividad. Al respecto, cabe decir que cada uno de los autores ha tenido plena libertad para elaborar sus comentarios de acuerdo con su propia área de conocimiento y punto de vista personal. No obstante, en general, se ha pretendido adoptar una metodología común que permite abordar de manera sistemática y, en la medida de lo posible, estandarizada, cada uno de los comentarios que conforman esta obra. Para esos efectos, las pautas generales para la elaboración de los comentarios parten de una estructura que comprende los antecedentes, la relevancia temática y contexto, el análisis del contenido del capítulo correspondiente, las conclusiones del autor y las referencias bibliográficas. Sin embargo, la pertinencia de incorporar cada uno de estos criterios y, fundamentalmente, el orden establecido para el análisis del contenido de cada capítulo ha quedado al arbitrio de los autores.

Para finalizar quiero dejar constancia de mi gratitud y reconocimiento a quienes conforman el Comité Editorial del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales tanto por la generosa invitación para coordinar este esfuerzo conjunto, como por el tiempo dedicado a la revisión y retroalimentación para mejorar el contenido de este

texto. Mención especial merece la comisionada Areli Cano quien impulsó de manera acuciosa la elaboración de este proyecto desde sus inicios, al igual que el comisionado Oscar Guerra Ford cuyo seguimiento y constante apoyo hicieron posible la culminación del mismo. De igual forma quiero manifestar mi profundo agradecimiento al Dr. Carlos Mata Prates, integrante del Comité Jurídico Interamericano (CJI) de la Organización de los Estados Americanos (OEA), y a cada uno de los autores, por su amplio compromiso con el fortalecimiento de una cultura en materia de protección de datos personales que redunde en beneficio de una sociedad cada vez más global y cercana a la tecnología.

**María Solange Maqueo**
**Coordinadora Editorial**

# PRÓLOGO

En las sociedades actuales encontramos diferentes demandas, no necesariamente novedosas pero sí más inmediatas, de los individuos —esencialmente pero no de manera exclusiva— acerca de la necesaria protección jurídica de diferentes valores considerados primarios e irrenunciables que hacen a la esencia de un Estado de derecho que se precie de tal.

Al respecto y vinculado a la materia de este texto preliminar debe hacerse referencia al derecho a la privacidad y protección de datos personales y al acceso a la información pública como dos elementos estructurales de una sociedad democrática. Cabe precisar que no nos encontramos ante dos concepciones contrapuestas o que persiguen finalidades diferentes, sino que son de naturaleza complementarias y, en algunos aspectos de las mismas, necesitadas de una delimitación precisa que implique un balance, una estimación de los valores que buscan preservar y que, en cada caso, será imprescindible proceder a su determinación. Dicho lo anterior debemos señalar que si bien estamos frente a institutos complementarios e intrínsecamente vinculados son diferentes y admiten un tratamiento separado (aunque no independiente o autárquico). En el caso del presente trabajo, que se pone a consideración de los operadores del derecho y público en general, pues se trata de un ejercicio que busca abarcar los diferentes aspectos del tema en consideración, nos detendremos en el derecho a la privacidad del cual el derecho a la protección de datos personales es una parte fundamental de la estructura de dicho instituto.

La importancia de este tema se ha reflejado en la recepción que realizan las normas de los derechos internos de los diferentes Estados. Es importante señalar que en algunos países el derecho a la protección de datos personales se encuentra recogido en la norma de mayor eficacia formal, es decir, la Constitución, de manera expresa —es el caso del derecho mexicano— o derivada de la interpretación evolutiva de la misma y, en otros, se establece el mismo mediante normas legislativas. A su vez, cabe destacar que en la mayoría de los países latinoamericanos el dictado de leyes sobre el derecho a la protección de datos personales se realizó en la última década.

En el ámbito del derecho internacional americano debe consignarse que la Asamblea General de la Organización de los Estados Americanos (OEA), mediante la resolución AG/RES. 2811 (XLIII-O/13), encomendó al Comité Jurídico

Interamericano (CJI) que formule propuestas a la Comisión de Asuntos Jurídicos y Políticos sobre las diferentes formas de regular la protección de datos personales, incluyendo un proyecto de Ley Modelo sobre Protección de Datos Personales, tomando en consideración los estándares internacionales alcanzados en la materia.

El CJI mediante la Resolución CJI/RES. 212 (LXXXVI-0/15) del 27 de marzo de 2015 dispuso: "Aprobar el informe del Comité Jurídico Interamericano 'Privacidad y protección de datos personales' documento CJI/doc. 474/15 rev.2, anexo a la presente Resolución. 3. Transmitir esta resolución al Consejo Permanente de la Organización de los Estados Americanos. 4. Dar por concluido los trabajos del Comité Jurídico Interamericano sobre este tema" (luego volveré sobre el punto 4, es decir, la conclusión del tema por parte del CJI).

Un primer aspecto a considerar refiere que el Comité Jurídico Interamericano se inclinó —teniendo en consideración la naturaleza del tema de estudio y el impacto que causan las nuevas tecnologías de la información— por una Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas. Tal como fue señalado en el mencionado informe:

> [la] finalidad de estos principios es instar a los Estados miembros de la organización a que adopten medidas para que se respete la privacidad, reputación y dignidad de las personas. Su propósito es servir de base para que los Estados miembros consideren la posibilidad de formular y adoptar leyes con objeto de proteger la información personal y los intereses en materia de privacidad de las personas en las Américas.

A su vez,

> [la] finalidad de los Principios de la OEA sobre la privacidad y la protección de datos personales es establecer un marco para salvaguardar los derechos de la persona a la protección de los datos personales y a la autodeterminación en lo que respecta a la información. Los principios se basan en normas reconocidas a nivel internacional. Su intención es proteger a las personas de la recopilación, el uso, la retención y la divulgación ilícitos o innecesarios de datos personales […]. Las normas relativas a la privacidad deben permitir que los consumidores y las empresas se beneficien del uso de datos personales de una manera segura y protegida. Deben ser equilibradas y tecnológicamente neutrales y permitir el libre flujo de datos dentro de cada país y a través de fronteras nacionales de una manera que fomente la innovación tecnológica y promueva el desarrollo económico y el crecimiento del comercio. Además de 1) proteger efectivamente la privacidad personal; 2) garantizar el libre flujo de datos para promover el progreso económico; por lo cual los

> Estados deben 3) aplicar una política clara de transparencia con respecto a sus protecciones y procedimientos.

El concepto de privacidad, tal como fue señalado

> [se encuentra] claramente establecido en el artículo V de la Declaración Americana de los Derechos y Deberes del Hombre (1948) y en los artículos 11 y 13 de la Convención Americana sobre Derechos Humanos (Pacto de San José) (1969) (apéndice A). La Corte Interamericana de Derechos Humanos ha confirmado el derecho a la privacidad.
>
> Además, la Constitución y las leyes fundamentales de muchos Estados miembros de la OEA garantizan el respeto y la protección de la privacidad, la dignidad personal y el honor familiar, la inviolabilidad del hogar y las comunicaciones privadas, los datos personales y conceptos conexos.
>
> […]
>
> Asimismo, los principios fundamentales de la libertad de expresión y de asociación y el libre flujo de información se reconocen en los principales sistemas de derechos humanos del mundo, entre ellos en el sistema de la OEA.

Por su parte el ámbito de aplicación abarca por igual a los órganos públicos y privados en relación con los datos generados, recopilados o administrados por los mismos. Con relación a los principios sobre la Protección de la Privacidad y los Datos Personales, éstos se resumen de la siguiente manera:

1) Propósitos legítimos y justos: Los datos personales deben ser recopilados solamente para fines legítimos y por medios justos y legales.

2) Claridad y consentimiento: Se deben especificar los fines para los cuales se recopilan los datos personales en el momento de proceder a su recopilación. Como regla general, los datos personales solamente deben ser recopilados con el consentimiento de la persona a que se refieran.

3) Pertinencia y necesidad: Los datos deben ser verídicos, pertinentes y necesarios para los fines expresos de su recopilación.

4) Uso limitado y retención: Los datos personales deben ser mantenidos y utilizados solamente de manera legítima y compatible con el fin o fines para los cuales se recopilaron. No deberán mantenerse más del tiempo necesario para su propósito o propósitos y de conformidad con la legislación nacional correspondiente.

5) Deber de confidencialidad: Los datos personales no deben divulgarse, ponerse a disposición de terceros ni emplearse para otros propósitos

que no sean aquellos para los cuales se obtuvieron, excepto con el conocimiento o consentimiento de la persona en cuestión o bajo la habilitación de la ley.

6) Protección y seguridad: Los datos personales deben ser protegidos mediante salvaguardias razonables y adecuadas contra accesos no autorizados, pérdida, destrucción, uso, modificación o divulgación.

7) Fidelidad de los datos: Los datos personales deben mantenerse fieles y actualizados hasta donde sea necesario para los propósitos de su uso.

8) Acceso y corrección: Se deben establecer métodos razonables para permitir que aquellas personas cuyos datos personales han sido recopilados puedan solicitar al contralor de datos que los modifique, corrija o elimine. En caso de disponerse la restricción a dicho acceso o corrección, deberán fundarse los motivos de cualquiera de estas restricciones de conformidad con la legislación nacional.

9) Datos personales sensibles: Algunos tipos de datos personales, teniendo en cuenta su sensibilidad en contextos particulares, son especialmente susceptibles de causar daños considerables a las personas si se hace mal uso de ellos. Los controladores de datos deberían adoptar medidas de privacidad y de seguridad que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los individuos sujetos de la información.

10) Responsabilidad: Los controladores de datos adoptarán e implementarán las medidas correspondientes para el cumplimiento de estos principios.

11) Flujo transfronterizo de datos y responsabilidad: Los Estados miembros cooperarán entre sí en la creación de mecanismos y procedimientos que aseguren que los controladores de datos que operen en más de una jurisdicción puedan ser efectivamente responsabilizados por el incumplimiento de estos principios.

12) Publicidad de las excepciones: Cuando las autoridades nacionales establezcan excepciones a estos principios por motivos relacionados con la soberanía nacional, la seguridad interna o externa, el combate a la criminalidad, el cumplimiento de normativas u otras prerrogativas de orden público, deben poner en conocimiento del público dichas excepciones.

La Resolución del Comité Jurídico Interamericano CJI/RES.212 (LXXXVI-O/15) que aprueba el informe que contiene los principios de la OEA sobre la Privacidad y Protección de Datos Personales dispuso en su numeral 4º “Dar por concluidos los trabajos del Comité Jurídico Interamericano sobre este tema”. No obstante, la evolución de la cuestión hizo necesario que el Comité dispusiera en su 92 período ordinario de sesiones, llevado a cabo del 26 de febrero al 2 de marzo de 2018 en la Ciudad de México, volverlo a incluir en su orden del día. Como fundamento

de la decisión se tuvo en consideración, entre otros aspectos, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos elaborados por la Red Iberoamericana de Protección de Datos Personales (RIPD), la nueva normativa de la Unión Europea sobre el tema, así como algunos hechos de notoriedad directamente vinculados a esta cuestión.

Es pertinente señalar que México ha tenido un desarrollo destacado en el tema de la privacidad y la protección de datos personales a partir o desde las modificaciones realizadas a su Constitución y desarrollado, posteriormente, por vía legislativa en línea con los principios establecidos por la OEA. Es en el marco de dicha realidad fáctica que se inscribe el estudio académico que tengo el honor de prologar y que constituye un trabajo notable por su profundidad y extensión, ya que abarca prácticamente todos los puntos que se vinculan a la privacidad y protección de los datos personales.

El estudio se titula *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Comentada* bajo la coordinación editorial de la jurista María Solange Maqueo Ramírez y en la que participan más de quince destacados juristas quienes analizan y comentan los diferentes títulos de la ley, lo cual hace evidente la importancia de la obra puesta a consideración del público en general y los operadores jurídicos en particular.

Una obra de esta envergadura pone o mejor aún mantiene a México como uno de los países de avanzada en la dogmática y doctrina acerca de la privacidad y la protección de datos personales y será un trabajo ineludible a la hora de acercarnos al estudio de esta temática con rigor y profundidad.

**Dr. Carlos Alberto Mata Prates**
**Miembro del Comité Jurídico Interamericano**

# SEMBLANZAS DE LOS AUTORES

**María Solange Maqueo**
**Coordinadora Editorial**

Doctora *summa cum laude* en el programa Estado de Derecho y Políticas Públicas de la Universidad de Salamanca, España. Cuenta con el Grado de Salamanca y la Cátedra *Jean Monnet* por esa misma universidad. Abogada egresada de la Escuela Libre de Derecho. Actualmente es profesora investigadora titular de la División de Estudios Jurídicos del Centro de Investigación y Docencia Económicas (CIDE), miembro del Sistema Nacional de Investigadores, distinción que otorga el Consejo Nacional de Ciencia y Tecnología (CONACYT), y del Comité Científico de la Editorial Tirant Lo Blanch, Ediciones de la Universidad de Salamanca (España), del Consejo Editorial de la revista académica *Estudios en Derecho a la Información* del Instituto de Investigaciones Jurídicas de la UNAM, del Consejo Consultivo de la Asociación Internet.MX (antes AMIPCI), del Consejo Asesor de la Red para la Rendición de Cuentas y presidenta del Consejo Consultivo del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Conferencista y autora de diversas publicaciones tanto nacionales como internacionales en materia de privacidad y protección de datos personales.

**María Mercedes Albornoz**

Doctora en derecho, egresada de la Université de Paris II, Panthéon-Assas, de París, Francia, donde también obtuvo un DEA (Diplôme d'Études Approfondies) en Derecho Internacional Privado y del Comercio Internacional. Previamente, se graduó como abogada en la Universidad Nacional del Litoral, localizada en Santa Fe, Argentina. Actualmente es profesora investigadora titular de la División de Estudios Jurídicos del Centro de Investigación y Docencia Económicas (CIDE). El Sistema Nacional de Investigadores la reconoce con el Nivel II. Su trabajo de investigación se concentra actualmente en el flujo transfronterizo de datos personales, el impacto de las tecnologías de la información y de la comunicación en el derecho internacional privado y la solución de controversias en línea. Colabora como asesora externa de la Secretaría de Relaciones Exteriores en materia de derecho internacional privado. Es miembro de la Asociación Americana de Derecho Internacional Privado y de la Academia Mexicana de Derecho Internacional Privado y Comparado.

### Alessandra Barzizza Vignau

Fue participante en la Escuela del Sur de Gobernanza de Internet de la Organización de los Estados Americanos (OEA). Cuenta con un Diplomado en Privacidad, Regulación y Gobernanza de Datos del Centro de Investigación y Docencia Económicas (CIDE) y un curso de Derecho Internacional Público impartido en la Academia de Derecho Internacional de La Haya. Egresada de la Licenciatura en Derecho del CIDE. Actualmente es consultora jurídica independiente en materia de ciberseguridad y gobernanza de internet. Fue Asistente de Proyecto de Investigación en la División de Estudios Jurídicos del CIDE en materia de privacidad y protección de datos personales y laboró en el área de derecho corporativo y financiero de la firma de abogados Müggenburg, Gorches y Peñalosa. Dos veces participante en el concurso “Phillip C. Jessup International Law Moot Court Competition”, donde obtuvo el premio de “mejor orador” a nivel nacional. Campeona nacional del “Concurso Nacional de Derecho Constitucional”.

### José Antonio Caballero Juárez

Doctor en derecho, egresado de la Universidad de Navarra, España. Maestro en derecho por la Universidad de Stanford y licenciado en derecho por la Universidad Nacional Autónoma de México (UNAM). Actualmente es profesor investigador titular de la División de Estudios Jurídicos del Centro de Investigación y Docencia Económicas (CIDE). El Sistema Nacional de Investigadores lo reconoce con el Nivel III. Ha sido profesor en diversas universidades e institutos de capacitación judicial. Ha publicado libros, capítulos de libros, ponencias y artículos sobre temas relacionados con la justicia, el federalismo y la protección de derechos.

### Mauricio Castillo Torres

Tiene un Diplomado en Privacidad, Regulación y Gobernanza de Datos impartido por el Centro de Investigación y Docencia Económicas (CIDE). Egresado de la Licenciatura en Derecho por esa misma institución. Ha formado parte de diversos proyectos de investigación en las materias constitucional y derechos humanos, autonomía e independencia presupuestal de las instituciones electorales, así como de diseño orgánico y facultades del ministerio de gobernación. Asimismo, ha participado en diversos litigios de relevancia nacional en las materias administrativa y constitucional. Actualmente se desempeña en el ámbito jurisdiccional en la Sala Superior del Tribunal Electoral del Poder Judicial de la Federación con la labor principal de elaborar proyectos de sentencia.

### Alfonso Cavazos Guajardo

Doctor en derecho con orientación en Derecho Constitucional y Gobernabilidad por la Facultad de Derecho y Criminología de la Universidad Autónoma de Nuevo León. Profesor investigador de la Universidad de Monterrey y candidato a investigador nacional del Sistema Nacional de Investigadores. Autor de diversos artículos y capítulos de libros, entre los que destacan *La transición centenaria del federalismo mexicano a la luz de las reformas constitucionales. De la descentralización a la concentración del poder público* y *Previa audiencia y el debido proceso. Su tutela tratándose de miembros de instituciones policiales*, así como *El principio de No Taxation without Representation, la migración y su impacto en los ordenamientos jurídicos latinoamericanos* y *Las garantías del debido proceso legal a favor de los migrantes en el Estado mexicano*, éstos en coautoría con el Dr. Michael G. Núñez Torres.

### Mónica Estrada Tanck

Abogada, egresada de la Escuela Libre de Derecho. Laboró por diez años en el sector público. En el IFAI (ahora INAI) fue subdirectora de Clasificación y Datos Personales, y directora de Análisis y Proyectos en la Oficina del entonces comisionado presidente del Instituto, Alonso Lujambio, en donde fue la encargada de integrar los expedientes y elaborar los proyectos de resolución de recursos de revisión en materia de acceso a la información y protección de datos personales. Fue coordinadora de asesores del secretario de Educación Pública. Ha sido catedrática universitaria en la Escuela Libre de Derecho y en la Universidad Nacional Autónoma de México en la materia de Derecho a la Información y Derecho Administrativo, y ha escrito diversos artículos sobre clasificación de información y datos personales. Actualmente es consultora jurídica independiente en materia de protección de datos personales, transparencia, acceso a la información y anticorrupción.

### Ana Elena Fierro

Doctora en derecho por el Instituto de Investigaciones Jurídicas de la UNAM. Maestra en derecho por la Universidad de Georgia, EE.UU. y maestra en Filosofía por la Universidad Anáhuac, campus Mayab. Licenciada en derecho por el ITAM. Actualmente es coordinadora de la Maestría en Administración y Políticas Públicas y profesora investigadora del CIDE. Sus líneas de investigación son: transparencia, rendición de cuentas y responsabilidad de servidores públicos. Entre sus publicaciones recientes destacan: *Responsabilidad de los servidores públicos. Del castigo a la confianza*, FCE; Título Cuarto. *De las responsabilidades de los servidores públicos, particulares*

*con faltas administrativas graves o hechos de corrupción, Constitución Política de los Estados Unidos Mexicanos Comentada*, José Ramón Cossío (Coord.); *Retos de los partidos políticos en transparencia proactiva para su publicación, The Rule of Law and Mexico´s energy reform, Part 2: Regulating The New Sector, ¿Accountability, transparency and responsability in Mexico*.

### Paulina del Pilar Gutiérrez

Abogada e internacionalista experta en temas de libertad de expresión, internet y uso de las tecnologías desde un enfoque de derechos humanos. Su experiencia profesional abarca proyectos de investigación y defensa de derechos humanos en los ámbitos nacional e internacional en Canadá, Guatemala, Estados Unidos y México. Actualmente es oficial del Programa de Derechos Digitales en ARTICLE 19 Oficina para México y Centroamérica; asesora en proyectos de telecomunicaciones, libertad de expresión y protección de datos desde la perspectiva latinoamericana y de género; miembro del Consejo Consultivo del Programa de DDHH en la organización estadounidense BENETECH, centrada en el uso de la tecnología para el empoderamiento y el bienestar social y conferencista internacional en foros de gobernanza de internet y derechos humanos.

### Olivia Andrea Mendoza

Doctora en derecho con distinción *ad honorem* por la Benemérita Universidad Autónoma de Puebla. Maestra en derecho con especialidad en Derecho Económico y licenciada en derecho por esa misma institución. Especialista en Derechos Humanos por la Universidad de Castilla-La Mancha. Actualmente es profesora investigadora titular de tiempo completo de INFOTEC (Centro Público CONACYT). Miembro del Sistema Nacional de Investigadores, Nivel I. Coordinadora académica y miembro del Núcleo Académico Básico de la Maestría en Derecho y TIC. Su línea de investigación es Regulación y Tecnología, particularmente relacionada con la protección de datos personales. Conferencista nacional e internacional y autora de diversos artículos académicos en dichas temáticas. Colaboradora del Observatorio Iberoamericano de Datos Personales. Vicepresidenta de Investigación de la Academia Multidisciplinaria de Derecho y Tecnologías AMDETIC. Profesora invitada de la División de Educación Continua de la Facultad de Derecho de la UNAM.

### Jimena Moreno González

Maestra en dirección internacional por el Instituto Tecnológico Autónomo de México. Abogada por la Universidad Nacional Autónoma de México con Diplomado en Políticas Públicas y en Competencia Económica por el Centro de Investigación y Docencia Económicas, cuenta con un curso de Derecho Constitucional Norteamericano por la Universidad de Berkeley, California. Actualmente se desempeña como secretaria general del CIDE y profesora de la División de Estudios Jurídicos de esa institución. Imparte cursos sobre transparencia, acceso a la información y protección de datos personales. Especialista en políticas públicas, dirección estratégica, datos personales y derecho internacional. La línea de investigación que actualmente desarrolla implica un área de inversiones, regulación vinculada a políticas públicas y su impacto regulatorio en los tres niveles de gobierno: federal, estatal y municipal, con especial énfasis en las recientes reformas constitucionales y datos personales. Coautora del *Manual de Derecho Internacional Público* y de artículos en revistas internacionales sobre inversiones, educación jurídica y protección de datos personales.

### Michael G. Núñez Torres

Doctor en derecho constitucional por la Universidad de Salamanca, España. Coordinador de Programas y Redes de Investigación Internacional de la Facultad de Derecho y Criminología de la Universidad Autónoma de Nuevo León. Profesor e investigador de la Facultad de Derecho y Criminología de esa misma Universidad. Miembro del Sistema Nacional de Investigadores, Nivel I. Miembro del cuerpo académico Derecho Constitucional y miembro del Consejo Consultivo Latinoamericano del Centro di studi sull´America Latina del Dipartimento di Scienze politiche e sociali dell´Università di Bologna. Actualmente es director consultivo y de Análisis Jurídicos de la Procuraduría General de Justicia del Estado de Nuevo León. Autor de libros y artículos científicos en revistas indexadas en editoriales nacionales e internacionales.

### Gisela María Pérez Fuentes

Doctora en derecho. Desde el año 2002 es profesora investigadora de tiempo completo en la Universidad Juárez Autónoma de Tabasco (UJAT). Pertenece al Sistema Nacional de Investigadores de CONACYT, Nivel III. Miembro de la Academia Mexicana de Ciencias desde 2014. Forma parte del Ilustre Colegio de Abogados de Madrid desde 1996 hasta la fecha, en la actualidad como no ejerciente. Imparte clases de licenciatura, maestría y doctorado en las materias Responsabilidad Civil, Persona, Derechos Reales, Metodología de la

Investigación y Derechos de Autor. Desde 2009 es líder del Cuerpo Académico Estudios de Derecho Civil en la UJAT, logrando el grado de consolidado. Pertenece a varios consejos de asesoría académica, investigación y comités editoriales en los ámbitos nacional e internacional. Desde 2012 es responsable académico del Doctorado de Estudios Jurídicos certificado por PNPC-CONACYT.

### José Luis Piñar Mañas

Doctor en derecho por la Universidad Complutense de Madrid y catedrático de Derecho Administrativo de las universidades de Castilla-La Mancha y CEU San Pablo de Madrid. Ha sido decano de las facultades de Derecho de ambas universidades y vicerrector de Relaciones Internacionales de la segunda. Ha sido director de la Agencia Española de Protección de Datos, vicepresidente del Grupo Europeo de Autoridades de Protección de Datos y presidente-fundador de la Red Iberoamericana de Protección de Datos. Fue *Adjunt Professor of Law* de la Universidad de Georgetown. Es vocal permanente y presidente de la sección de Derecho Público de la Comisión General de Codificación. Miembro de la Comisión Jurídica del Consejo General de la Abogacía Española y del Consejo Asesor de la Asociación Española de Fundaciones. Director del Master Oficial Universitario en Protección de Datos, Transparencia y Acceso a la Información de la Universidad CEU San Pablo. Titular de la Cátedra Google sobre Privacidad, Sociedad e Información, constituida en esa misma universidad. Abogado y consultor internacional en protección de datos.

### Oscar R. Puccinelli

Doctor en derecho constitucional egresado de la Universidad de Buenos Aires, Argentina. Doctor y profesor *honoris causa* en diversas universidades latinoamericanas. Profesor de posgrados de las universidades Panamericana (México) y de San Carlos (Guatemala). Profesor de Derecho Constitucional, Derecho Procesal Constitucional y Derechos Humanos en las facultades de Derecho de las universidades Nacional y Católica Argentina (Rosario). Especialista en derecho de la información (en particular, en protección de datos personales, acceso a la información pública y libertad de expresión). Participó en alrededor de 300 eventos como conferencista. Se desempeñó en diversos cargos públicos y actualmente es juez de la Cámara de Apelación en lo Civil y Comercial de Rosario. Entre sus libros específicos sobre derecho a la información destacan *Habeas data en Iberoamérica* (Temis, Bogotá, 1999), *Protección de datos de carácter personal* (Astrea, Buenos Aires, 2004) y *Juicio de habeas data* (Hammurabi, Buenos Aires, 2016).

## Miguel Recio Gayo

Maestro internacional universitario en Protección de Datos, Transparencia y Acceso a la Información por la Universidad CEU San Pablo de Madrid. Maestro en derecho de la propiedad intelectual por The George Washington University Law School. Actualmente se desempeña como abogado especializado en materia de protección de datos personales y privacidad. Forma parte del claustro de profesores del Máster Internacional Universitario en Protección de Datos, Transparencia y Acceso a la Información por la Universidad CEU San Pablo de Madrid. Es autor de varias obras sobre derecho digital, protección de datos personales y otras materias tanto en México como en España. Ha ganado varios premios de investigación jurídica en materia de derecho digital.

## Nelson Remolina Angarita

Profesor de la Facultad de Derecho de la Universidad de los Andes (Bogotá, Colombia). Director de la Especialización en Derecho Comercial. Doctor *summa cum laude* en Ciencias Jurídicas de la Pontificia Universidad Javeriana. Master of Laws del London School of Economics and Political Sciences. Especialista en Derecho Comercial y abogado de la Universidad de los Andes. Cofundador (2001) y director del Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones e Informática (GECTI) http://gecti.uniandes.edu.co/ de la Facultad de Derecho de la Universidad de los Andes. Fundador (2008) y director del Observatorio Ciro Angarita Barón sobre la Protección de Datos Personales en Colombia http://habeasdatacolombia.uniandes.edu.co/. Ganador del Premio Internacional Protección de Datos Personales de Investigación 2014, conferido por la Agencia Española de Protección de Datos (AEPD) sobre trabajos originales e inéditos que traten acerca del derecho a la protección de datos en países iberoamericanos.

## Andrés Velázquez

Presidente y fundador de MaTTica, primer laboratorio en investigaciones digitales de América Latina. Especialista en seguridad informática y cómputo forense, posicionado en el medio como uno de los expertos con mayor experiencia por su participación resolviendo casos para organizaciones privadas y entidades como la Interpol, la ONU y múltiples agencias gubernamentales. La revista de negocios *Expansión* lo nombró recientemente como uno de los 30 jóvenes en los treinta para liderar el cambio en México. Fungió como embajador ejecutivo para la Asociación Internacional de Investigadores de Alta Tecnología (HTCIA) y consultor del Consejo de Europa en el proyecto GLACY (Global

Action on Cybercrime) para América Latina. Coautor del libro *Normatividad Bancaria 2017*. Cuenta con certificaciones en Seguridad Informática como la Certified Information Systems Security Professional (CISSP) y la Infosec Evaluation Methodology (IEM) otorgada por la Agencia de Seguridad de los Estados Unidos, así como en las principales herramientas especializadas para investigaciones digitales.

# REFERENCIA DE SIGLAS Y ACRÓNIMOS

| | |
|---|---|
| **AEPD** | Agencia Española de Protección de Datos. |
| **APEC** | Foro de Cooperación Económica Asia Pacífico. |
| **CIAPDP** | Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. |
| **Convenio 108** | Convenio No. 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. |
| **CADH** | Convención Americana sobre Derechos Humanos (Pacto de San José). |
| **CPEUM** | Constitución Política de los Estados Unidos Mexicanos. |
| **Derechos ARCO** | Derechos de acceso, rectificación, cancelación y oposición. |
| **DOF** | Diario Oficial de la Federación. |
| **IFAI** | Instituto Federal de Transparencia, Acceso a la Información y Protección de Datos. |
| **INAI** | Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. |
| **LFPDPPP** | Ley Federal de Protección de Datos Personales en Posesión de los Particulares. |
| **LFTAIP** | Ley Federal de Transparencia y Acceso a la Información Pública. |
| **LFTAIPG** | Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. |

| | |
|---|---|
| **LGPDPPSO** | Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. |
| **LORTAD** | Ley Orgánica de Regulación y Tratamiento Automatizado de Datos. |
| **LGTAIP** | Ley General de Transparencia y Acceso a la Información Pública. |
| **OCDE** | Organización para la Cooperación y el Desarrollo Económicos. |
| **OEA** | Organización de los Estados Americanos. |
| **ONU** | Organización de las Naciones Unidas. |
| **RGPD** | Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). |
| **RIPD** | Red Iberoamericana de Protección de Datos. |
| **TJUE** | Tribunal de Justicia de la Unión Europea. |
| **UE** | Unión Europea. |

# TÍTULO PRIMERO
# DISPOSICIONES GENERALES

# CAPÍTULO I
# DEL OBJETO DE LA LEY

***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.*

*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.*

*En todos los demás supuestos diferentes a los mencionados en el párrafo anterior, las personas físicas y morales se sujetarán a lo previsto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.*

***Artículo 2.*** *Son objetivos de la presente Ley:*

*I. Distribuir competencias entre los Organismos garantes de la Federación y las Entidades Federativas, en materia de protección de datos personales en posesión de sujetos obligados;*

*II. Establecer las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, mediante procedimientos sencillos y expeditos;*

*III. Regular la organización y operación del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales a que se refieren esta Ley y la Ley General de Transparencia y Acceso a la Información Pública, en lo relativo a sus funciones para la protección de datos personales en posesión de sujetos obligados;*

*IV. Garantizar la observancia de los principios de protección de datos personales previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia;*

*V. 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;*

*VI. Garantizar que toda persona pueda ejercer el derecho a la protección de los datos personales;*

*VII. Promover, fomentar y difundir una cultura de protección de datos personales;*

*VIII. Establecer los mecanismos para garantizar el cumplimiento y la efectiva aplicación de las medidas de apremio que correspondan para aquellas conductas que contravengan las disposiciones previstas en esta Ley, y*

*IX. Regular los medios de impugnación y procedimientos para la interposición de acciones de inconstitucionalidad y controversias constitucionales por parte de los Organismos garantes locales y de la Federación, de conformidad con sus facultades respectivas.*

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

*I. Áreas: Instancias de los sujetos obligados previstas en los respectivos reglamentos interiores, estatutos orgánicos o instrumentos equivalentes, que cuentan o puedan contar, dar tratamiento, y ser responsables o encargadas de los datos personales;*

*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;*

*III. Bases de datos: Conjunto ordenado de datos personales referentes a una persona física identificada o identificable, condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización;*

*IV. Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponda;*

*V. Comité de Transparencia: Instancia a la que hace referencia el artículo 43 de la Ley General de Transparencia y Acceso a la Información Pública;*

*VI. Cómputo en la nube: Modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente;*

*VII. Consejo Nacional: Consejo Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales a que se refiere el artículo 32 de la Ley General de Transparencia y Acceso a la Información Pública;*

*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;*

*XII. Días: Días hábiles;*

*XIII. Disociación: El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo;*

*XIV. Documento de seguridad: Instrumento que describe y da cuenta de manera general sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee;*

*XV. Encargado: La persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable;*

*XVI. Evaluación de impacto en la protección de datos personales: Documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable;*

*XVII. Fuentes de acceso público: Aquellas bases de datos, sistemas o archivos que por disposición de ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación, tarifa o contribución. No se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a las disposiciones establecidas por la presente Ley y demás normativa aplicable;*

*XVIII. Instituto: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el cual es el organismo garante de la Federación en materia de protección de datos personales en posesión de los sujetos obligados;*

*XIX. Medidas compensatorias: Mecanismos alternos para dar a conocer a los titulares el aviso de privacidad, a través de su difusión por medios masivos de comunicación u otros de amplio alcance;*

*XX. Medidas de seguridad: Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales;*

*XXI. Medidas de seguridad administrativas: Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales;*

*XXII. Medidas de seguridad físicas: Conjunto de acciones y mecanismos para proteger el entorno físico de los datos personales y de los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:*

*a) Prevenir el acceso no autorizado al perímetro de la organización, sus instalaciones físicas, áreas críticas, recursos e información;*

*b) Prevenir el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, recursos e información;*

*c) Proteger los recursos móviles, portátiles y cualquier soporte físico o electrónico que pueda salir de la organización, y*

*d) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento eficaz, que asegure su disponibilidad e integridad;*

*XXIII. Medidas de seguridad técnicas: Conjunto de acciones y mecanismos que se valen de la tecnología relacionada con hardware y software para proteger el entorno digital de los datos personales y los recursos involucrados en su tratamiento. De manera enunciativa más no limitativa, se deben considerar las siguientes actividades:*

*a) Prevenir que el acceso a las bases de datos o a la información, así como a los recursos, sea por usuarios identificados y autorizados;*

*b) Generar un esquema de privilegios para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;*

*c) Revisar la configuración de seguridad en la adquisición, operación, desarrollo y mantenimiento del software y hardware, y*

*d) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales;*

*XXIV. Organismos garantes: Aquellos con autonomía constitucional especializados en materia de acceso a la información y protección de datos personales, en términos de los artículos 6o. y 116, fracción VIII de la Constitución Política de los Estados Unidos Mexicanos;*

*XXV. Plataforma Nacional: La Plataforma Nacional de Transparencia a que hace referencia el artículo 49 de la Ley General de Transparencia y Acceso a la Información Pública;*

*XXVI. Programa Nacional de Protección de Datos Personales: Programa Nacional de Protección de Datos Personales;*

*XXVII. Remisión: Toda comunicación de datos personales realizada exclusivamente entre el responsable y encargado, dentro o fuera del territorio mexicano;*

*XXVIII. Responsable: Los sujetos obligados a que se refiere el artículo 1 de la presente Ley que deciden sobre el tratamiento de datos personales;*

*XXIX. Sistema Nacional: El Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;*

*XXX. Supresión: La baja archivística de los datos personales conforme a la normativa archivística aplicable, que resulte en la eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable;*

*XXXI. Titular: La persona física a quien corresponden los 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*

*XXXIV. Unidad de Transparencia: Instancia a la que hace referencia el artículo 45 de la Ley General de Transparencia y Acceso a la Información Pública.*

***Artículo 4.*** *La presente Ley será aplicable a cualquier tratamiento de datos personales que obren en soportes físicos o electrónicos, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización.*

***Artículo 5.*** *Para los efectos de la presente Ley, se considerarán como fuentes de acceso público:*

*I. Las páginas de Internet o medios remotos o locales de comunicación electrónica, óptica y de otra tecnología, siempre que el sitio donde se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general;*

*II. Los directorios telefónicos en términos de la normativa específica;*

*III. Los diarios, gacetas o boletines oficiales, de acuerdo con su normativa;*

*IV. Los medios de comunicación social, y*

*V. Los registros públicos conforme a las disposiciones que les resulten aplicables.*

*Para que los supuestos enumerados en el presente artículo sean considerados fuentes de acceso público será necesario que su consulta pueda ser realizada por cualquier persona no impedida por una norma limitativa, o sin más exigencia que, en su caso, el pago de una contra prestación, derecho o tarifa. No se considerará una fuente de acceso público cuando la información contenida en la misma sea o tenga una procedencia ilícita.*

***Artículo 6.*** *El Estado garantizará la privacidad de los individuos y deberá velar por que 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.*

***Artículo 7.*** *Por regla general no podrán tratarse datos personales sensibles, salvo que se cuente con el consentimiento expreso de su titular o en su defecto, se trate de los casos establecidos en el artículo 22 de esta Ley.*

*En el tratamiento de datos personales de menores de edad se deberá privilegiar el interés superior de la niña, el niño y el adolescente, en términos de las disposiciones legales aplicables.*

***Artículo 8.*** *La aplicación e interpretación de la presente Ley se realizará conforme a lo dispuesto en la Constitución Política de los Estados Unidos Mexicanos, los Tratados Internacionales de los que el Estado mexicano sea parte, así como las resoluciones y sentencias vinculantes que emitan los órganos nacionales e internacionales especializados, favoreciendo en todo tiempo el derecho a la privacidad, la protección de datos personales y a las personas la protección más amplia.*

*Para el caso de la interpretación, se podrán tomar en cuenta los criterios, determinaciones y opiniones de los organismos nacionales e internacionales, en materia de protección de datos personales.*

***Artículo 9.*** *A falta de disposición expresa en la presente Ley, se aplicarán de manera supletoria las disposiciones del Código Federal de Procedimientos Civiles y de la Ley Federal de Procedimiento Administrativo.*

*Las leyes de las Entidades Federativas, en el ámbito de sus respectivas competencias, deberán determinar las disposiciones que les resulten aplicables en materia supletoria a los Organismos garantes en la aplicación e interpretación de esta Ley.*

## COMENTARIO

**María Solange Maqueo**

### I. Antecedentes

Las disposiciones generales previstas en este primer capítulo dan cuenta del cúmulo de experiencias en nuestro sistema jurídico que han llevado a un grado de especialización y precisión lingüística del derecho a la protección de datos personales. Como puede observarse en su texto, el contenido de este capítulo adopta y clarifica algunos conceptos que se han venido gestando desde su propia recepción en nuestro sistema jurídico, fundamentalmente a partir de la LFTAIPG de 2002, la LFPDPPP de 2010, su Reglamento de 2011 y demás disposiciones normativas tanto en el ámbito federal como estatal. A todo lo cual se añade la utilización de referentes internacionales de vanguardia en la materia a los que nuestro país no ha sido ajeno.

Aunado a lo anterior, el presente capítulo materializa la reforma constitucional de 2014 en materia de protección de datos personales por medio de la definición de su objeto, ámbito personal de aplicación y adopción de otras medidas que permitan su congruencia con el régimen aplicable al sector privado, la naturaleza del INAI como órgano constitucional autónomo y su propio carácter de derecho humano.

### II. Relevancia temática y contexto

Bajo una adecuada técnica legislativa, en este primer capítulo relativo a las Disposiciones Generales se establecen los preceptos que deberán guiar el alcance y la interpretación de la totalidad del contenido de la LGPDPPSO y de su ulterior desarrollo normativo. Se trata, pues, de los preceptos que permiten clarificar, precisar y, en cierta forma, especializar su contenido. Para esos efectos, las disposiciones generales comprenden la naturaleza y el ámbito de aplicación de la ley, los conceptos que utiliza, los criterios para su interpretación, el régimen de supletoriedad y los límites o excepciones del derecho humano a la protección de datos personales. En ese sentido, las disposiciones generales

se constituyen en referencia obligada para la comprensión y aplicación de esta ley con independencia de la temática concreta que se pretenda abordar.

## III. Análisis del contenido

A efecto de sistematizar el contenido de este capítulo, a continuación se presenta el desarrollo de cada uno de los citados elementos comprendidos en las disposiciones generales previstas en la presente ley.

**1. Naturaleza de la ley.** El primer párrafo del artículo 1 de la LGPDPPSO establece que la misma "es de orden público y de observancia general en toda la República". Con ello se adopta una fórmula legislativa comúnmente utilizada para destacar la importancia de la dimensión pública y colectiva del propio ordenamiento frente a los intereses privados que se derivan del mismo. Como han puesto de manifiesto nuestros tribunales, "el orden público constituye […] una garantía de la sociedad para que las personas y autoridades ejerzan razonablemente sus derechos dentro del Estado y no sólo consiste en el mantenimiento de la tranquilidad y bienestar colectivo, sino también conlleva la armonía social en cuanto al legítimo ejercicio de los derechos, libertades y poderes dentro del Estado; esto es, la coexistencia pacífica entre el poder y la libertad".[1] Además, en términos prácticos la característica de orden público de la ley implica una cierta abstracción de su contenido respecto del ámbito propio de la autonomía de la voluntad, donde sus disposiciones adquieren un carácter imperativo más que supletorio.

Por otra parte, la observancia general de la LGPDPPSO no sólo la dota de validez para todo el territorio mexicano, de manera consistente con su carácter concurrente, sino que además supone su aplicabilidad o acatamiento por todo aquel que se coloque en los supuestos normativos previstos por el propio ordenamiento. La intención manifiesta de esta ley para generar estándares homogéneos en todo el país sólo es susceptible de cumplirse a través de esta generalidad en su observancia.

Finalmente, de acuerdo con este primer párrafo del artículo 1 de la LGPDPPSO se trata de una ley reglamentaria de los artículos 6º, Base A, y 16, segundo párrafo, de la CPEUM. Ello implica que esta ley general desarrolla de manera directa dos preceptos constitucionales que, sólo en un análisis en conjunto, constituyen el reconocimiento al más alto nivel normativo del derecho humano a la protección de datos personales.

**2. Objeto de la ley.** De conformidad con el párrafo cuarto del artículo 1 de la LGPDPPSO, ésta tiene por objeto establecer bases, principios y procedimientos

[1] Cuarto Tribunal Colegiado en Materia Administrativa del Primer Circuito (diciembre 2012). Tesis I.4o.A.11 K (10ª.), Décima Época, *Semanario Judicial de la Federación y su Gaceta*, Libro XV. Tomo II, p. 1575.

comunes, aplicables para cualquier persona en su carácter de titular de datos personales, órgano garante o sujeto obligado previsto por la propia ley (esto es, cualquier autoridad, entidad, órgano y organismo de los tres poderes, órganos autónomos, partidos políticos, fideicomisos y fondos públicos) en cualquiera de los tres órdenes de gobierno. Se trata, pues, de un ordenamiento jurídico que pretende, por una parte, establecer altos estándares para la protección de los datos personales en posesión de los sujetos obligados y, por la otra, que dichos estándares resulten aplicables en todo el territorio nacional, sin distinción de la naturaleza, características o jurisdicción de los órganos e instituciones gubernamentales.

**3. Ámbito de aplicación.** Cabe precisar que, a diferencia de lo que ocurre en materia de transparencia y acceso a la información pública, los sindicatos y las personas físicas o morales que reciban y ejerzan recursos públicos o que realicen actos de autoridad, no son considerados como sujetos obligados en términos de esta ley general y, por ende, tampoco lo deben ser en términos de las legislaciones estatales aplicables conforme a la misma. Lo cual no implica que no puedan constituirse en responsables del tratamiento de datos personales, sino que su régimen jurídico aplicable está previsto en la LFPDPPP. Esta decisión legislativa de excluir del régimen propio del sector público a los sindicatos y a las personas físicas o morales antes aludidas, atiende a la necesidad de evitar duplicidades o regímenes diferenciados que pudieran ser aplicables a los mismos.

En términos del párrafo segundo del artículo 1 de la LGPDPPSO, sus disposiciones “son de aplicación y observancia directa para los sujetos obligados pertenecientes al orden federal”. Ello supone, al menos, dos dimensiones diferenciadas de esta ley. Una dirigida a desarrollar el contenido y los procesos para el ejercicio del derecho a la protección de datos personales con una aplicación directa a los órganos de gobierno del orden federal (y, por excepción, a las entidades federativas que omitan la expedición de una ley propia y armonizada) y, otra, cuyo objeto sea efectivamente regular un régimen de facultades constitucionalmente concurrentes que explican su carácter de ley *general*.

Mientras que la primera de estas dimensiones infiere que no es necesario emitir una ley federal en materia de protección de datos personales en posesión de los sujetos obligados, toda vez que la propia ley *general* cumple de manera directa con esta función; la segunda, explica el carácter general de la ley en el sentido de materializar el cambio en el régimen de facultades que introdujo la reforma constitucional de 2014, a fin de pasar de un esquema tradicional de distribución de competencias y facultades reservadas propias del federalismo, tal como se establece en el artículo 124 constitucional, a uno de carácter concurrente. Este régimen de facultades concurrentes supone, a su vez, que

tanto las entidades federativas como la Federación pueden actuar respecto de una misma materia, en este caso, sobre la protección de datos personales en posesión de los sujetos obligados, pero es a través de esta ley general que emite el Congreso de la Unión en la que se determina "la forma y los términos de la participación de dichos entes […]".[2] De ahí que las legislaturas locales se han visto en la necesidad de armonizar su propia legislación estatal conforme a las disposiciones previstas por la ley general.

**4. Objetivos.** En consonancia con lo anterior, esta ley general establece en su artículo 2 los objetivos que persigue, mismos que pueden agruparse fundamentalmente en tres funciones: (1) Establecer estándares y objetivos comunes de protección que constituyan pisos mínimos y condiciones homogéneas en el tratamiento de los datos personales y el ejercicio de los derechos que lo dotan de efectividad; (2) distribuir competencias entre la Federación y las entidades federativas, en una relación jerárquica o de división competencial y (3) establecer mecanismos de coordinación que permitan la participación conjunta de la Federación y las entidades federativas a través de la creación del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y, cabría agregar, la generación de esquemas de planeación y programación compartida y congruente entre sí, mediante el Programa Nacional de Protección de Datos Personales.

**5. Conceptos.** Por su parte, el artículo 3 de la LGPDPPSO establece diversos conceptos que atienden a funcionalidades distintas. Mientras que en algunos casos se trata de conceptos fundamentales que se encuentran en la propia base de construcción del derecho a la protección de datos personales y que, por ende, se tornan indispensables para su interpretación y determinación de su alcance y configuración; otros, atienden a precisar y abreviar las referencias que sobre ellos se establecen en el propio texto de la ley.

Entre los primeros cabe destacar en un primer momento el concepto de *datos personales*, previsto en la fracción IX del artículo 3 de la LGPDPPSO. Se trata de un concepto muy amplio que implica la concurrencia de dos elementos: por una parte, el dato o información, cualquiera que éste sea, con independencia de su naturaleza, contenido o tipo de soporte que lo comprenda; y, por la otra, su relación o vínculo con una persona física que permite (de manera directa o indirecta) su singularización frente a las demás. Este concepto se construye a partir de la concurrencia de cuatro componentes interrelacionados entre sí: (1) cualquier información, (2) concerniente (3) a una persona física (4) que la identifica o que, bajo criterios de razonabilidad, la

[2] FACULTADES CONCURRENTES EN EL SISTEMA JURÍDICO MEXICANO. SUS CARACTERÍSTICAS GENERALES. Suprema Corte de Justicia de la Nación (enero 2002). Tesis Jurisprudencial P./J. 142/2001, Novena Época, *Semanario Judicial de la Federación y su Gaceta*. Tomo XV, p. 1042.

hace identificable.[3] Cabe destacar que tanto en la propia definición de datos personales, como en la definición de titular que introduce la fracción XXXI del artículo 3 de la propia ley, sólo las personas físicas son consideradas como titulares de los datos personales, cerrando así el debate generado en torno a la posibilidad de que este régimen jurídico pudiera ser aplicable para las personas morales o jurídicas.

La fracción X del artículo 3 de la LGPDPPSO distingue una categoría especial de datos personales, denominados *datos personales sensibles*, a fin de elevar algunos de sus estándares de protección (por ejemplo, en las formas de expresar el consentimiento por parte del titular de los datos personales) o limitar, en la medida de lo posible, su tratamiento (como lo dispone el primer párrafo del artículo 7 de esta ley). Así pues, se trata, en términos de la propia ley, de aquella información personal que se refiere a la esfera más íntima del titular o que pudiera dar origen a discriminación o conlleve un riesgo grave para éste. Cabe decir que la enumeración que introduce la ley sobre esta categoría especial de datos personales (esto es, aquellos que pudieran revelar aspectos como el origen racial o étnico, el estado de salud, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual) sólo tiene un carácter enunciativo mas no limitativo. Ello genera espacios para la interpretación sobre la categorización de otros datos personales que, si bien por su propia naturaleza no son necesariamente datos sensibles, pudieran llegar a serlo en razón del tratamiento y la finalidad que se persigue con el mismo, tales como los datos biométricos.

Adicionalmente, cabe decir que los datos personales que han pasado por un proceso de disociación, esto es, que en términos de la fracción XIII del artículo 3 de la LGPDPPSO ya "no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo", dejan de ser considerados como tales. Sin embargo, su eficacia depende de los resultados obtenidos, que deben ser similares o equivalentes a la eliminación o borrado de los datos personales, sin perder de vista los posibles riesgos residuales de la reidentificación ante las tecnologías disponibles. Algunos ejemplos de procesos de disociación son la aleatorización o la privacidad diferencial que si bien suponen el tratamiento de datos personales, su utilización tiene por objeto disociar de manera irreversible o definitiva la información de su titular, a fin de que éste no pueda ser identificado o identificable.[4]

---

[3] Cfr. Grupo de Trabajo del Artículo 29. (2007). *Dictamen 4/2007 sobre el concepto de datos personales, 01248/ES WP 136.* Adoptado el 20 de junio. [Archivo PDF]. Disponible en: http://www.redipd.es/actividades/encuentros/VI/common/wp136_es.pdf, [fecha de consulta: 30 de abril 2018].

[4] Cfr. Montaña, C. y Rodríguez, B. (2017). *Criterios de Disociación de Datos Personales*. Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento. Aprobado por el Consejo Ejecutivo de la Unidad Reguladora y Control de Datos Personales de Uruguay, Resolución núm. 68/017, de 26 de abril.

Otro de los conceptos fundamentales del derecho a la protección de datos personales es el que corresponde al *tratamiento*. Constituye un término amplio que implica cualquier gestión y decisión de destino sobre la información personal. De conformidad con lo dispuesto por la fracción XXXIII del artículo 3 de la LGPDPPSO, el tratamiento incluye cualquier actividad relacionada con el ciclo de vida de un dato personal, desde su recogida, almacenamiento, uso, circulación, hasta su propia supresión, esto es, su "eliminación, borrado o destrucción de los datos personales bajo las medidas de seguridad previamente establecidas por el responsable" (fracción XXX del propio artículo 3).

En ciertas circunstancias, cuando se ha cumplido la finalidad para la cual fueron recabados los datos personales o, incluso, cuando se ha ejercido el derecho de cancelación por parte del titular de los datos y éste resulta procedente, el sujeto obligado puede impedir el tratamiento de los mismos sin proceder de manera inmediata a su supresión o borrado físico "con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas". Este procedimiento se denomina *bloqueo* conforme a la fracción IV del artículo 3 de la LGPDPPSO y supone, así, un período de conservación de los datos personales sin que los mismos puedan ser tratados (con excepción del almacenamiento o, incluso, posible acceso de persona alguna)[5] para finalidades distintas a una posible responsabilidad derivada de la relación jurídica entre el responsable del tratamiento y el titular de los datos personales. En una interpretación sistemática con lo dispuesto por los artículos 23 y 24 de la propia ley general, el bloqueo también podría ser procedente para cumplir con los plazos de conservación de los datos personales previstos imperativamente en ley, cuando éstos hayan cumplido las finalidades para las cuales fueron recabados.[6]

Por otra parte, cabe advertir que entre los conceptos comprendidos por el artículo 3 de la LGPDPPSO se establecen importantes distinciones que implican, a su vez, un régimen diferenciado de cumplimiento de la normatividad en la materia. Es el caso de las fracciones XXVIII y XV que distinguen entre el responsable y el encargado del tratamiento de datos personales, respectivamente. Mientras que el responsable es quien toma las decisiones sobre el tratamiento de los datos personales (por ejemplo, en su uso, finalidades, tipos de soporte, transferencias, etc.); el encargado, quien es ajeno a la organización del responsable, actúa a cuenta y nombre del mismo. En ese sentido, la figura de encargado se configura a través de la formalización

[5] Dozo, D. y Martínez, P. (2013). *Glosario Iberoamericano de Protección de Datos*, XVII Edición de los Premios Protección de Datos Personales. Madrid: Agencia Española de Protección de Datos, p. 20.

[6] Agencia Española de Protección de Datos. (2001). *Bloqueo de datos de carácter personal - Año 2001* [Archivo PDF]. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/derecho_acceso_rectificacion_cancelacion_oposicion/common/pdfs/2001-0000_Bloqueo-de-datos-de-car-aa-cter-personal.pdf, [fecha de consulta: 30 de abril 2018].

de la relación jurídica con el responsable, quien establece los términos del tratamiento mediante la celebración de un convenio, contrato o cualquier otro instrumento jurídico aplicable en el que consten las condiciones específicas del tratamiento. En el supuesto de que el encargado no se ajustara a los términos establecidos por el responsable adquiriría para sí, el carácter de responsable del tratamiento de los datos personales. La ley general destina todo un capítulo a fin de regular esta situación.

En relación con lo anterior, las fracciones XXXIII y XXVII del artículo 3 de la LGPDPPSO distinguen entre transferencia y remisión de datos personales, respectivamente. Si bien en ambos casos suponen una transmisión o comunicación de la información personal de un sujeto a otro, sea en el ámbito nacional o internacional, las transferencias se realizan del responsable del tratamiento de datos personales a otro responsable del tratamiento, mientras que las remisiones se ejecutan del responsable del tratamiento al encargado de los mismos en los términos previstos en el párrafo anterior. Cabe decir que el concepto de transferencia ha sido objeto de análisis desde los propios orígenes del derecho a la protección de datos personales. Su régimen jurídico no sólo se sitúa en el ámbito nacional, sea en esta ley general para el sector público o en la LFPDPPP para el sector privado, sino también en el ámbito internacional. Entre los instrumentos internacionales que la comprenden cabe mencionar las Directrices de la OCDE de 1980, el Convenio 108 y su Protocolo Adicional del Consejo de Europa, la Resolución 45/95 del 14 de diciembre de 1990 de la Asamblea General de Naciones Unidas y el Marco de Privacidad APEC de 2004, por citar sólo algunos de ellos.[7]

Por otra parte, uno de los pilares en la propia construcción del derecho a la protección de datos personales es precisamente el *consentimiento* del titular. Éste se encuentra definido en la fracción VIII del artículo 3, 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". Las formas para expresar el consentimiento —sea expreso o tácito—, su desarrollo como principio, así como sus excepciones se encuentran desarrolladas por el propio texto de la ley general. De tal forma que si bien el consentimiento por parte del titular de los datos personales se configura en la regla general para habilitar y, con ello, legitimar el tratamiento de los mismos, existen supuestos de excepción previstos de manera taxativa por la propia ley general en los cuales no se requiere.

Precisamente dentro de las excepciones al consentimiento se encuentra otro de los conceptos previstos por el artículo 3, fracción XVII de la LGPDPPSO,

[7] Remolina, N. (2015). *Recolección internacional de datos personales: un reto del mundo post-internet*. XVIII Edición del Premio Protección de Datos Personales de Investigación de la Agencia Española de Protección de Datos. Madrid: AEPD/Agencia Estatal, Boletín Oficial del Estado.

esto es, el relativo a las *fuentes de acceso público* concebidas como "aquellas bases de datos, sistemas o archivos que por disposición de la ley puedan ser consultadas públicamente cuando no exista impedimento por una norma limitativa y sin más exigencia que, en su caso, el pago de una contraprestación o contribución".

Al respecto, el artículo 5 de la propia LGPDPPSO establece de manera taxativa cuáles se consideran fuentes de acceso público, entre las que incluye internet, directorios telefónicos, registros públicos, medios de comunicación social, entre otros. Pero en cualquier caso se excluyen de las mismas, aquellas que tienen una procedencia ilícita o cuyo contenido se considera ilícito. Cabe decir que el carácter de fuente de acceso público si bien constituye una excepción para recabar el consentimiento de los titulares de los datos personales en ellas contenidos, no exime a quien trata dichos datos personales del cumplimiento de las disposiciones normativas aplicables en materia de protección de datos personales.

Otra de las definiciones que incorpora el artículo 3 en su fracción II es la relativa a los *avisos de privacidad*. Se trata del medio *ad hoc*, cualquiera que sea el formato en el que se presente, para informar al titular de los datos personales sobre la existencia, alcance y propósitos del tratamiento de sus datos. En otras palabras, el aviso de privacidad se constituye en el medio idóneo a través del cual el responsable del tratamiento de los datos personales o sujeto obligado cumple con el principio de información del derecho a la protección de datos personales y posibilita el ejercicio de los derechos ARCO (llamados así por la fracción XI del artículo 3 de la LGPDPPSO en referencia a los derechos de acceso, rectificación, cancelación y oposición).

Si bien el aviso de privacidad debe ponerse a disposición del titular de los datos personales de manera personal o directa, a partir del momento en el cual se recaban sus datos personales, el propio artículo 3, en su fracción XIX, introduce la posibilidad de que dicha puesta a disposición se realice a través de medios masivos de comunicaciones. Se trata, pues, de las llamadas *medidas compensatorias*, mismas que adquieren un carácter excepcional para dar a conocer o comunicar el aviso de privacidad, ante la presencia de una imposibilidad material o alguna dificultad que suponga un esfuerzo desproporcionado de entregarlo personal o directamente al titular.

Por lo que se refiere a las *medidas de seguridad*, el artículo 3 de la LGPDPPSO, en su fracción XX, las define como el "conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales". Se trata de uno de los deberes jurídicos para los sujetos obligados más relevante para dotar de verdadera efectividad al derecho a la protección de datos personales, toda vez que implica

la adopción de diversos controles que permitan "proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado",[8] esto es, garantizar "la confidencialidad, integridad y disponibilidad de los datos personales". Si bien la ley general distingue entre distintos tipos de medidas de seguridad, sean físicas, técnicas o administrativas, su adecuación dependerá del tipo de datos que se traten, los soportes en los que se contienen y los esquemas organizacionales de cada sujeto obligado. El cumplimiento de este deber jurídico por parte de los sujetos obligados no sólo se efectúa a través de su adopción efectiva, sino que es necesario que las mismas consten en el llamado *documento de seguridad* (fracción XIV del artículo 3 de la LGPDPPSO). Dada su relevancia, la ley general dedica todo un capítulo específico para regular las mismas.

**6. Límites del derecho humano a la protección de datos personales.** Ahora bien, el artículo 6 de la LGPDPPSO, establece que "el Estado garantizará la privacidad de los individuos y deberá velar porque terceras personas no incurran en conductas que puedan afectarla arbitrariamente". Con ello, esta ley general no sólo reconoce el carácter instrumental del derecho a la protección de datos personales para dotar de efectividad a la privacidad de las personas físicas, sino que además, enfatiza las obligaciones positivas del Estado mexicano para proteger y garantizar los derechos humanos, de conformidad con lo dispuesto por el artículo 1º de la CPEUM.

De igual forma, el artículo 6 de la LGPDPPSO, en su segundo párrafo, retoma lo dispuesto por el artículo 16, segundo párrafo, de la CPEUM, en el cual se establecen los límites del derecho humano a la protección de datos personales, a saber, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. Con ello no sólo se reitera que esta ley general es reglamentaria tanto del artículo 6º, apartado A, como del 16, segundo párrafo, de la Constitución, como se señala en el artículo 1 de la propia LGPDPPSO, sino que además implica el reconocimiento de que el derecho humano a la protección de datos personales no es absoluto pues está sujeto a límites establecidos taxativamente por la propia norma constitucional y cuyo desarrollo sólo es factible a través de disposiciones con rango de ley, esto es, bajo el llamado principio de reserva de ley.

**7. Aplicación e interpretación de la ley.** El artículo 8 de la LGPDPPSO, relativo a la aplicación e interpretación del propio ordenamiento jurídico, reitera la necesidad de adoptar una interpretación de nuestro ordenamiento jurídico a partir de la CPEUM, los tratados internacionales de los que México sea parte y las resoluciones y sentencias vinculantes que emitan los órganos nacionales e internacionales

[8] Dozo, D. y Martínez, P. (2013). *Glosario Iberoamericano de Protección de Datos*, XVII Edición de los Premios Protección de Datos Personales. Madrid: Agencia Española de Protección de Datos, p. 74.

especializados. Así pues, este precepto jurídico más que presentar un contenido propio, replica lo dispuesto por el párrafo segundo del artículo 1º constitucional en el sentido de que "[l]as normas relativas a los derechos humanos se interpretarán de conformidad con esta Constitución y con los tratados internacionales de la materia favoreciendo en todo tiempo a las personas la protección más amplia." Se trata, pues, de la llamada *interpretación conforme*, en la cual el principio pro persona debe orientar el sentido de la interpretación hacia la preferencia de la norma más protectora para el individuo.[9] Asimismo, este precepto de la ley general reconoce la posibilidad de adoptar criterios, determinaciones y opiniones de organismos nacionales e internacionales en calidad de referentes para la interpretación de este ordenamiento jurídico. Ello resulta de particular relevancia en el tema de la protección de datos personales, toda vez que su desarrollo y configuración en el sistema jurídico mexicano ha seguido en buena medida el diseño y construcción del derecho en la Unión Europea, además, por supuesto, de la necesidad de generar estándares homogéneos con un alcance global ante el advenimiento de la era digital.[10]

Además, en congruencia con lo anterior, cabe destacar lo dispuesto por el segundo párrafo del artículo 7 de la LGPDPPSO, de conformidad con el cual "en el tratamiento de datos personales de menores de edad se deberá privilegiar el interés superior de la niña, el niño y el adolescente, en términos de las disposiciones legales aplicables." Ello supone la aplicación del principio del interés superior de la niñez (también llamado interés superior del menor o de los niños, niñas y adolescentes), previsto en el párrafo noveno del artículo 4º de la CPEUM, conforme al cual deben orientarse todas las decisiones y actuaciones del Estado. En términos de la Suprema Corte de Justicia de la Nación, el interés superior del menor no sólo se constituye como un principio jurídico interpretativo fundamental, sino también como un derecho sustantivo y como una norma de procedimiento.[11]

En términos de nuestro máximo tribunal, el interés superior del menor,

> ... implica que el desarrollo de [los niños, niñas y adolescentes]… y el ejercicio pleno de sus derechos deben ser considerados como criterios rectores para la elaboración de normas y la aplicación de éstas en todos los órdenes relativos a su vida. Así las autoridades deben asegurar y garantizar

[9] Cfr. Rodríguez, G. *et al*. (2013). *Interpretación Conforme. Metodología para la Enseñanza. La Reforma Constitucional en Materia de Derechos Humanos*. México: SCJN/OACNUDH/CDHDF. [Archivo PDF]. Disponible en: http://www2.scjn.gob.mx/red/coordinacion/archivos_Interpretacion.pdf, [fecha de consulta: 30 de abril 2018].

[10] Cfr. Maqueo, M., Moreno, J. y Recio, M. (2017). Protección de Datos Personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario, *Revista de Derecho (Valdivia)*, vol. 30, núm. 1, pp. 77-96. Disponible en: http://www.scielo.cl/scielo.php?script=sci_abstract&pid=S0718-09502017000100004&lng=es&nrm=iso, [fecha de consulta: 30 de abril 2018].

[11] Derechos de las niñas, niños y adolescentes. El interés superior del menor se erige como la consideración primordial que debe atenderse en cualquier decisión que les afecte. Suprema Corte de Justicia de la Nación. Tesis 2ª. CXLI/2016 (10ª.), Décima Época, *Semanario Judicial de la Federación y su Gaceta*, Libro 28, enero de 2017, Tomo I, p. 796.

> que en todos los asuntos, decisiones y políticas públicas en las que se les involucre, todos los niños, niñas y adolescentes tengan el disfrute y goce de todos sus derechos humanos, especialmente de aquellos que permiten su óptimo desarrollo, […]. En ese sentido, el principio del interés superior del menor de edad implica que la protección de sus derechos debe realizarse por parte de las autoridades a través de medidas reforzadas o agravadas en todos los ámbitos que estén relacionados directa o indirectamente con los niños, niñas y adolescentes, ya que sus intereses deben protegerse siempre con una mayor intensidad.[12]

Este principio, sin duda alguna, cobra especial relevancia en materia de protección de datos personales, toda vez que constituyen un sector de la población especialmente vulnerable y expuesto a los riesgos que supone el desarrollo y utilización de las tecnologías de la información y comunicación. En ese sentido se constituye tanto en un criterio interpretativo al momento de aplicar la normativa en la materia como en un objetivo claro de política pública.

**8. Régimen de supletoriedad.** Finalmente, el artículo 9 de la LGPDPPSO establece el carácter supletorio del Código Federal de Procedimientos Civiles y de la Ley Federal de Procedimiento Administrativo para la aplicación o la interpretación de todas aquellas cuestiones que no se encuentren previstas por la propia ley general. Esta disposición se explica a partir de la primera dimensión a la que nos hemos referido anteriormente sobre el carácter de esta ley general en el sentido de que tiene una aplicación directa para los órganos de gobierno federales. No obstante, tratándose de una ley que regula facultades concurrentes, la aplicación supletoria de estos ordenamientos no opera para las entidades federativas, las cuales pueden subsanar algunas omisiones de la LGPDPPSO en sus propias legislaciones o prever sus propias leyes estatales supletorias. Cabe decir que en la práctica esta disposición puede presentar algunas dificultades en cuanto a su aplicación, ya que establece dos ordenamientos con carácter supletorio sin considerar parámetros que permitan identificar cuál de ellos sería preferible en caso de una contradicción. En cualquier caso habría que relacionarlo con la interpretación conforme y el principio pro persona, a que se refiere el artículo 8 de esta ley general.

## IV. Conclusiones

Como se advierte en este primer capítulo de la LGPDPPSO, se trata de un ordenamiento jurídico de vanguardia que adopta elevados estándares para la protección de datos personales. Sin embargo, dado el propio carácter amplio

[12] INTERÉS SUPERIOR DE LOS MENORES DE EDAD. NECESIDAD DE UN ESCRUTINIO ESTRICTO CUANDO SE AFECTEN SUS INTERESES. Suprema Corte de Justicia de la Nación (septiembre de 2016). Tesis jurisprudencial P./J. 7/2016, Décima Época, *Semanario Judicial de la Federación y su Gaceta*, Libro 34, Tomo I, p. 10.

de los conceptos comprendidos, la complejidad que en sí mismo supone un régimen de facultades concurrentes y su relevancia como ley reglamentaria de un derecho humano, se abren importantes espacios para la interpretación de sus disposiciones y la generación de criterios que brinden certeza jurídica tanto para los sujetos obligados como para los titulares de los datos personales.

## Referencias

Agencia Española de Protección de Datos. (2001). *Bloqueo de datos de carácter personal - Año 2001* [Archivo PDF]. Disponible en: http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/derecho_acceso_rectificacion_cancelacion_oposicion/common/pdfs/2001-0000_Bloqueo-de-datos-de-car-aa-cter-personal.pdf, [fecha de consulta: 30 de abril 2018].

Cuarto Tribunal Colegiado en Materia Administrativa del Primer Circuito (diciembre 2012). Tesis I.4o.A.11 K (10ª.), Décima Época, *Semanario Judicial de la Federación y su Gaceta*, Libro XV. Tomo II, p. 1575.

Dozo, D. y Martínez, P. (2013). *Glosario Iberoamericano de Protección de Datos, XVII edición de los Premios Protección de Datos Personales*. Madrid: Agencia Española de Protección de Datos, p. 20.

Grupo de Trabajo del Artículo 29. (2007). *Dictamen 4/2007 sobre el concepto de datos personales, 01248/ES WP 136*. Adoptado el 20 de junio. [Archivo PDF]. Disponible en: http://www.redipd.es/actividades/encuentros/VI/common/wp136_es.pdf, [fecha de consulta: 30 de abril 2018].

Maqueo, M., Moreno, J. y Recio, M. (2017). Protección de Datos Personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario, *Revista de Derecho (Valdivia)*, vol. 30, núm. 1, pp. 77-96. Disponible en: http://www.scielo.cl/scielo.php?script=sci_abstract&pid=S0718-09502017000100004&lng=es&nrm=iso, [fecha de consulta: 30 de abril 2018].

Montaña, C. y Rodríguez, B. (2017). *Criterios de Disociación de Datos Personales*. Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento. Aprobado por el Consejo Ejecutivo de la Unidad Reguladora y Control de Datos Personales de Uruguay, Resolución núm. 68/017, de 26 de abril.

Remolina, N. (2015). *Recolección internacional de datos personales: un reto del mundo post-internet. XVIII Edición del Premio Protección de Datos*

*Personales de Investigación de la Agencia Española de Protección de Datos*. Madrid: AEPD/Agencia Estatal, Boletín Oficial del Estado.

Rodríguez, G. *et al.* (2013). *Interpretación Conforme. Metodología para la Enseñanza. La Reforma Constitucional en Materia de Derechos Humanos*. México: SCJN/OACNUDH/CDHDF. [Archivo PDF]. Disponible en: http://www2.scjn.gob.mx/red/coordinacion/archivos_Interpretacion.pdf, [fecha de consulta: 30 de abril 2018].

Suprema Corte de Justicia de la Nación (enero 2002). Tesis jurisprudencial P./J. 142/2001, Novena Época, *Semanario Judicial de la Federación y su Gaceta*. Tomo XV, p. 1042.

Suprema Corte de Justicia de la Nación (enero 2017). Tesis 2ª CXLI/2016 (10ª.), Décima Época, *Semanario Judicial de la Federación y su Gaceta*, Libro 28. Tomo I, p. 796.

Suprema Corte de Justicia de la Nación (septiembre 2016).Tesis jurisprudencial P./J. 7/2016 (10ª.), Décima Época, *Semanario Judicial de la Federación y su Gaceta*, Libro 34, Tomo I, p. 10.

# CAPÍTULO II
# DEL SISTEMA NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

***Artículo 10.*** *El Sistema Nacional 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.*** *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.*

*Este esfuerzo conjunto e integral, aportará a la implementación de políticas públicas con estricto apego a la normatividad aplicable en la materia; el ejercicio pleno y respeto del derecho a la protección de datos personales y la difusión de una cultura de este derecho y su accesibilidad.*

***Artículo 12.*** *Además de los objetivos previstos en la Ley General de Transparencia y Acceso a la Información Pública, el Sistema Nacional tendrá como objetivo diseñar, ejecutar y evaluar un Programa Nacional de Protección de Datos Personales que defina la política pública y establezca, como mínimo, objetivos, estrategias, acciones y metas para:*

*I. Promover la educación y una cultura de protección de datos personales entre la sociedad mexicana;*

*II. Fomentar el ejercicio de los derechos de acceso, rectificación, cancelación y oposición;*

*III. Capacitar a los sujetos obligados en materia de protección de datos personales;*

*IV. Impulsar la implementación y mantenimiento de un sistema de gestión de seguridad a que se refiere el artículo 34 de la presente Ley, así como promover la adopción de estándares nacionales e internacionales y buenas prácticas en la materia, y*

*V. Prever los mecanismos que permitan medir, reportar y verificar las metas establecidas.*

*El Programa Nacional de Protección de Datos Personales, se constituirá como un instrumento rector para la integración y coordinación del Sistema Nacional, y deberá determinar y jerarquizar los objetivos y metas que éste debe cumplir, así como definir las líneas de acción generales que resulten necesarias.*

*El Programa Nacional de Protección de Datos Personales deberá evaluarse y actualizarse al final de cada ejercicio anual y definirá el conjunto de actividades y proyectos que deberán ser ejecutados durante el siguiente ejercicio.*

***Artículo 13.*** *El Sistema Nacional contará con un Consejo Nacional. En la integración, organización, funcionamiento y atribuciones del Consejo Nacional se estará a lo dispuesto por la Ley General de Transparencia y Acceso a la Información Pública y demás disposiciones aplicables.*

***Artículo 14.*** *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;*

*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, y*

*XXI. Las demás que se establezcan en otras disposiciones en la materia para el funcionamiento del Sistema Nacional.*

***Artículo 15.*** *El Consejo Nacional funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y demás ordenamientos aplicables.*

## COMENTARIO

**José Antonio Caballero Juárez**

### I. Antecedentes

Los artículos sobre los que se ocupa el presente comentario corresponden al Capítulo II de la LGPDPPSO, denominado *Del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*. El Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales fue creado con motivo de la publicación de la LGTAIP, publicada en el DOF el 4 de mayo de 2015. Los artículos del Capítulo II de la LGPDPPSO reenvían a la LGTAIP en lo que se refiere a la organización del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

A diferencia de otros sistemas nacionales, el de transparencia, acceso a la información pública y protección de datos personales no tiene sustento constitucional. No obstante, su creación en ley general le otorga un alcance nacional. Ello derivado de la forma en la que la Suprema Corte de Justicia de la Nación se ha pronunciado respecto de la jerarquía de las leyes generales en el orden jurídico mexicano.[13] El

[13] Si bien muy cuestionado, el criterio que prevalece es el siguiente: TRATADOS INTERNACIONALES. SON PARTE INTEGRANTE DE LA LEY SUPREMA DE LA UNIÓN Y SE UBICAN JERÁRQUICAMENTE POR ENCIMA DE LAS LEYES GENERALES, FEDERALES Y LOCALES. INTERPRETACIÓN DEL ARTÍCULO 133 CONSTITUCIONAL. Suprema Corte de Justicia de la Nación. (abril 2007). Tesis P. IX/2007, Novena Época, *Semanario Judicial de la Federación y su Gaceta*. Tomo XXV, p. 6.

artículo 28 de la LGTAIP señala en forma general las partes que integran al sistema y se refiere a su objetivo principal: fortalecer la rendición de cuentas del Estado mexicano. Ahí mismo destaca sus funciones de coordinación y evaluación de las acciones relativas a la política transversal de transparencia, acceso a la información y protección de datos personales, así como establecer e implementar criterios y lineamientos en la materia.

El artículo 29 de la LGTAIP se refiere a la herramienta operativa principal del sistema. Se trata de la coordinación. Es decir, de todas aquellas acciones que de manera consensuada se pueden adoptar entre las autoridades de los tres niveles de gobierno con el objeto de generar información, mejorar la gestión y el proceso de la información que se recaba y custodia, promover el acceso a la información y una cultura de transparencia y accesibilidad. De esta manera, el sistema reconoce explícitamente la estructura federal del Estado mexicano y busca facilitar la cooperación entre las autoridades federales, estatales y municipales para fortalecer los derechos de acceso a la información pública y protección de datos personales.

El artículo 30 se refiere a las partes integrantes del sistema. Al efecto, señala al INAI, los organismos garantes de las entidades federativas, la Auditoría Superior de la Federación, el Archivo General de la Nación y el Instituto Nacional de Estadística y Geografía. El artículo 32 se refiere a la integración de un Consejo Nacional del Sistema. A esta instancia pertenecen todos los integrantes del sistema y es regida por el presidente del INAI. El Consejo es la instancia política básica del sistema. La instancia operativa está en manos de un secretario ejecutivo encargado del funcionamiento ordinario del sistema y del seguimiento de las decisiones del Consejo.

## II. Relevancia temática y contexto

El Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales representa otra expresión sobre la forma en la que se pretende articular la acción de los tres niveles de gobierno en el marco del sistema federal mexicano para el cumplimiento de diversas funciones consideradas relevantes. Así, podemos encontrar sistemas nacionales en una diversidad de materias.[14] La mayor parte de ellos creados en los últimos años. Los sistemas nacionales tienen como objetivo principal mejorar la colaboración entre los tres niveles de gobierno en el desarrollo de una materia en concreto. Sin embargo, en muchos casos, también corresponde a los sistemas constituirse en mecanismos que facilitan el flujo de información, diseño y ejecución de políticas públicas, así como la evaluación de las mismas. En prácticamente todos los casos los sistemas

[14] Sistema Nacional de Salud, Sistema Nacional de Seguridad Pública, Sistema Nacional de Evaluación Educativa, Sistema Nacional Anticorrupción o el Sistema Nacional de Información Estadística y Geográfica, por mencionar algunos.

cuentan con ciertas atribuciones regulatorias. Los alcances y las características de las atribuciones regulatorias de los sistemas son muy variables.

En el caso del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales se trata de dar un nuevo impulso a las políticas orientadas a fomentar el acceso a la información pública, la rendición de cuentas y la protección de datos personales. Estas acciones no pueden entenderse sin relacionarse con dos cuestiones relevantes. La primera es el reciente desarrollo constitucional de acciones encaminadas a abatir la corrupción. Desde esta perspectiva, el acceso a la información pública y, sobre todo, la rendición de cuentas, se tornan fundamentales para la construcción de administraciones honestas y responsables en los tres niveles de gobierno. En este contexto, el Sistema Nacional de Transparencia cumple con una función de apoyo y fortalecimiento de una política nacional en la materia. La segunda tiene que ver con la protección de datos personales. La complejidad técnica que implica la implementación de acciones orientadas a la protección de datos personales exige que existan vías claras de colaboración entre las diversas instancias gubernamentales. Pero también que se desarrollen y difundan herramientas y mecanismos que permitan que los tres niveles de gobierno puedan cumplir con sus labores en forma satisfactoria.

## III. Análisis del contenido

**1. Funciones del Sistema Nacional de Transparencia.** El artículo 10 de la LGPDPPSO señala que, en materia de protección de datos personales en poder de sujetos obligados, el sistema tendrá como funciones coordinar y evaluar políticas de protección de datos, y establecer e implementar criterios y lineamientos sobre la materia. De esta manera, el artículo 10 establece en forma general dos tipos de función para el sistema en el ámbito de la protección de datos personales. Por una parte, le atribuye funciones de coordinación. Estas funciones se desarrollan con mayor claridad en algunas fracciones del artículo 14. Ahí se detallan labores de promoción, homologación de criterios (fracción VIII), análisis (fracción III) o de promoción (fracciones I y II). En cuanto a la fijación de criterios y lineamientos en la materia, las fracciones VI y IX (XIX) señalan que el sistema puede formular, establecer y ejecutar políticas generales sobre protección de datos.

A la luz de lo anterior, el Sistema Nacional de Transparencia aparece como una instancia nacional que tiene como propósito fundamental contribuir para que todos los organismos responsables de la protección de datos personales en el país cumplan con sus funciones. En particular, aquellos que tienen como función regular a los sujetos obligados. Así, el sistema aparece como una instancia encargada de generar y difundir información sobre el

funcionamiento de sus diversos integrantes. Además, colabora con ellos en la identificación de mejores prácticas y en la adopción de criterios que incidan en el perfeccionamiento de sus servicios.

Como función adicional, la ley le otorga al sistema ciertas funciones de carácter regulatorio. Es precisamente esta cuestión la que será desarrollada a lo largo del presente comentario.

El Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales fue creado en la LGTAIP. Este ordenamiento señala la forma en la que el Sistema estará organizado y establece las funciones que tendrá dicho Sistema en materia de transparencia y acceso a la información. Los artículos 13 y 15 de la ley en comento, refieren precisamente a la LGTAIP en lo que respecta a la integración y funcionamiento del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Esta cuestión fue abordada en el apartado de antecedentes del presente comentario.

Si bien desde el punto de vista legislativo las funciones de transparencia y acceso a la información pública se encuentran separadas de las de protección de datos personales, cuando se trata de sujetos obligados, la cuestión se encuentra estrechamente entrelazada. Así, toda política de transparencia o de acceso a la información pública necesariamente debe articularse con respecto a la protección de datos personales, tal y como lo establece la fracción II del apartado A del artículo 6º constitucional.

**2. Interacciones entre los actores del Sistema Nacional de Transparencia.** En el escenario antes descrito, es necesario caracterizar las interacciones que se producen entre los diversos actores que intervienen dentro del Sistema. Para tal efecto, debe tomarse en cuenta el esquema de distribución del poder vigente en el marco de la Constitución mexicana. Así, en materia de transparencia, acceso a la información pública y protección de datos personales en poder de sujetos obligados, encontramos que existen tres ámbitos: el de la Federación establecido en el artículo 6º apartado A, el de los estados de la República contenido en la fracción VIII del artículo 116 constitucional y el de la Ciudad de México en el artículo 122, apartado A, fracción VII. Para los tres casos se dispone establecer instituciones con autonomía constitucional encargadas de regular tanto la transparencia y el acceso a la información pública como la protección de datos personales en materia de sujetos obligados. Estos organismos tienen una naturaleza dual en el sentido de que poseen ciertas atribuciones de corte reglamentario y también realizan funciones, materialmente jurisdiccionales, para conocer recursos de revisión en contra de resoluciones en donde se niegue acceso a la información a particulares o se

susciten controversias en relación con el ejercicio de este derecho o el de la protección de datos personales.

Con base en el anterior esquema, corresponde a cada uno de los tres ámbitos antes mencionados generar las leyes necesarias para regular las materias de transparencia, acceso a la información y protección de datos personales en poder de sujetos obligados. Sin embargo, la regulación que emitan deberá ajustarse al contenido del artículo 6º de la CPEUM y, adicionalmente, a las leyes generales en la materia que emita el Congreso de la Unión en términos del artículo 73, fracción XXIX-S, de la propia Constitución.

Adicionalmente, es necesario considerar el carácter nacional del organismo federal en el sentido que de acuerdo con el párrafo quinto de la fracción VIII del apartado A, del artículo 6º constitucional, el Instituto federal puede conocer de los recursos de revisión que se presenten en contra de resoluciones emitidas por autoridades de las entidades federativas. Es decir, existe una especie de *certiorai* en materia de transparencia, acceso a la información y protección de datos personales en poder de sujetos obligados, que permite al organismo federal ejercer una especie de jurisdicción nacional en la materia. Sin lugar a dudas, se trata de una facultad de corte excepcional que permite la intervención de una institución federal en atribuciones que son competencia original de las entidades federativas.

**3. Alcances del Sistema Nacional de Transparencia.** El análisis de los alcances del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en poder de sujetos obligados necesariamente debe seguir los anteriores criterios de distribución de competencias establecidos tanto en la CPEUM como en las leyes generales de la materia.

Si bien la LGTAIP y la LGPDPPSO crean el Sistema Nacional, es necesario preguntarse cuáles pueden ser los alcances de semejante creación normativa. Como primera cuestión hay que considerar que la Suprema Corte de Justicia de la Nación ha sostenido que es posible que una ley general distribuya competencias entre la Federación, las entidades federativas y los municipios.[15] Ahora bien, en el caso de la ley en comento y de la General de Transparencia y Acceso a la Información se crea el Sistema, se le asignan diversas funciones y se le otorgan ciertas competencias regulatorias. En el caso de las funciones de

[15] Aquí un criterio reciente derivado de la controversia constitucional 71/2009: TURISMO. EL ARTÍCULO 1, PÁRRAFO PRIMERO, ÚLTIMA PARTE, DE LA LEY GENERAL RELATIVA, AL ESTABLECER QUE LA INTERPRETACIÓN EN EL ÁMBITO ADMINISTRATIVO DE ESE ORDENAMIENTO CORRESPONDE AL EJECUTIVO FEDERAL, A TRAVÉS DE LA SECRETARÍA DE TURISMO, NO TRANSGREDE LOS ARTÍCULOS 49 Y 89, FRACCIÓN I, CONSTITUCIONALES NI VIOLA LA AUTONOMÍA E INDEPENDENCIA DEL JEFE DE GOBIERNO DEL DISTRITO FEDERAL. Suprema Corte de Justicia de la Nación. (junio 2014). Tesis P. XXXIV/2014, Décima Época, *Semanario Judicial de la Federación y su Gaceta*, Libro 7. Tomo I, p. 159.

coordinación no parece haber problemas, toda vez que este tipo de acciones suelen sustentarse en el cumplimiento voluntario por parte de los diversos ámbitos involucrados. Al efecto, se suele emplear la vía convencional. Las propias leyes generales que nos ocupan, así lo reconocen.

La pregunta está en el tema de las atribuciones regulatorias del Sistema. Aquí se requiere determinar si una ley general puede no sólo distribuir competencias sino también crear nuevas entidades a las que les otorga atribuciones regulatorias con alcances tanto para la Federación como para las entidades federativas. De estimarse viable el arreglo en cuestión, la Federación y las entidades federativas están obligadas a seguir regulación proveniente de tres niveles: el constitucional, el de las leyes generales y el del sistema. Esta cuestión puede observarse en sistemas como el de Salud o el de Seguridad Pública. En otras materias, esta cuestión opera cuando se otorgan atribuciones regulatorias a organismos constitucionales autónomos. Tal es el caso del Instituto Federal de Telecomunicaciones o de la Comisión Federal de Competencia Económica.[16] Sin embargo, cabe hacer notar que se trata de regulación en materias que son federales. Es decir, la regulación no tiene efectos transversales sobre los órdenes de gobierno.

Desde luego que la creación de un Sistema Nacional de Transparencia con el propósito de ordenar y regular una materia no es novedosa. Sin embargo, cabe señalar que a diferencia del sistema que nos ocupa, otros tienen un sustento claramente constitucional. Tal es el caso del Sistema Nacional de Seguridad Pública contenido en el artículo 21 párrafo décimo de la Constitución. En este caso, el texto constitucional expresamente le otorga facultades regulatorias.

Por lo tanto, la existencia de atribuciones regulatorias a favor del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales requiere necesariamente de un criterio interpretativo más amplio del que hasta el momento ha sostenido la Suprema Corte de Justicia de la Nación en materia de federalismo. Si bien la tendencia reciente de nuestro Alto Tribunal ha sido ensanchar las atribuciones nacionales y federales frente a las de las entidades federativas, los avances siempre han sido razonablemente cautelosos. Con una óptica menos enfocada en la jerarquía normativa, es posible dar un carácter cuasi regulatorio a la normativa que se genere en el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Esta técnica se suele emplear para dar

[16] ESTADO REGULADOR. EL MODELO CONSTITUCIONAL LO ADOPTA AL CREAR A ÓRGANOS AUTÓNOMOS EN EL ARTÍCULO 28 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS. Suprema Corte de Justicia de la Nación (enero 2016). Tesis jurisprudencial P./J. 46/2015, Décima Época, *Semanario Judicial de la Federación y su Gaceta*, Libro 26, Tomo I, p. 339.

un carácter orientativo y persuasivo a las disposiciones normativas, pero sin llegar a constituir elementos integrantes del sistema normativo. Se trata de la creación de estándares que se entienden como buenas prácticas en una materia determinada y cuyo seguimiento puede entenderse como un elemento necesario para una operación eficaz. De esta manera, la alternativa de la cuasi regulación puede evitar los problemas de distribución de competencias que conlleva la regulación dura y, al mismo tiempo, sentar una base sólida para armonizar el funcionamiento de las instancias competentes en la materia.

## IV. Conclusiones

En el caso del sistema que nos ocupa, se percibe un alto grado de dificultad para el reconocimiento de sus atribuciones regulatorias. A pesar de ello, el sistema dista mucho de ser una estructura débil. Sus atribuciones para facilitar la colaboración a nivel nacional lo colocan como un mecanismo con alcances cuasi regulatorios. En ese sentido, si el sistema opera correctamente y sus posicionamientos cuentan con el respaldo técnico necesario, será muy difícil para cualquier organismo federal o las entidades federativas separarse de los mismos. En consecuencia, la función regulatoria se cumplirá más que por la amenaza de la coacción por el peso del prestigio del mecanismo que emite el estándar técnico en cuestión.

## Referencias

DOF. (1917). Constitución Política de los Estados Unidos Mexicanos, última reforma publicada el 15 de septiembre de 2017, *Diario Oficial de la Federación*.

DOF. (2015). Ley General de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*.

DOF. (2016). Ley Federal de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*.

DOF. (2017). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, *Diario Oficial de la Federación*.

Suprema Corte de Justicia de la Nación. (abril 2007). Tesis P. IX/2007, Novena Época, *Semanario Judicial de la Federación y su Gaceta*, Tomo XXV, p. 6.

Suprema Corte de Justicia de la Nación. (junio 2014). Tesis P. XXXIV/2014 (10ª.), *Semanario Judicial de la Federación y su Gaceta*, Libro 7. Tomo I, p. 159.

Suprema Corte de Justicia de la Nación. (diciembre 2015). Tesis jurisprudencial P./J. 45/2015 (10ª.), *Semanario Judicial de la Federación y su Gaceta*, Libro 25, Tomo I, p. 38.

Suprema Corte de Justicia de la Nación. (enero 2016). Tesis jurisprudencial P./J. 46/2015 (10ª.), *Semanario Judicial de la Federación y su Gaceta*, Libro 26, Tomo I, p. 339.

Suprema Corte de Justicia de la Nación. (enero 2016). Tesis jurisprudencial P./J. 47/2015 (10ª.), *Semanario Judicial de la Federación y su Gaceta*, Libro 26, Tomo I, p. 444.

# TÍTULO SEGUNDO
# PRINCIPIOS Y DEBERES

# CAPÍTULO I
# DE LOS PRINCIPIOS

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

***Artículo 17.*** *El tratamiento de datos personales por parte del responsable deberá sujetarse a las facultades o atribuciones que la normatividad aplicable le confiera.*

***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.*

***Artículo 19.*** *El responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad.*

***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.*

***Artículo 21.*** *El consentimiento podrá manifestarse de forma expresa o tácita. Se deberá entender que el consentimiento es expreso cuando la voluntad del titular se manifieste verbalmente, por escrito, por medios electrónicos, ópticos, signos inequívocos o por cualquier otra tecnología.*

*El consentimiento será tácito cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario.*

*Por regla general será válido el consentimiento tácito, salvo que la ley o las disposiciones aplicables exijan que la voluntad del titular se manifieste expresamente.*

*Tratándose de datos personales sensibles el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica o cualquier mecanismo de autenticación que al efecto se establezca, salvo en los casos previstos en el artículo 22 de esta Ley.*

***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.*

***Artículo 23.*** *El responsable deberá adoptar las medidas necesarias para mantener exactos, completos, correctos y actualizados los datos personales en su posesión, a fin de que no se altere la veracidad de éstos.*

*Se presume que se cumple con la calidad en los datos personales cuando éstos son proporcionados directamente por el titular y hasta que éste no manifieste y acredite lo contrario.*

*Cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones que resulten aplicables, deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos.*

*Los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales.*

***Artículo 24.*** *El responsable deberá establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleve a cabo, en los cuales se incluyan los periodos de conservación de los mismos, de conformidad con lo dispuesto en el artículo anterior de la presente Ley.*

*En los procedimientos a que se refiere el párrafo anterior, el responsable deberá incluir mecanismos que le permitan cumplir con los plazos fijados para la supresión de los datos personales, así como para realizar una revisión periódica sobre la necesidad de conservar los datos personales.*

***Artículo 25.*** *El responsable sólo deberá tratar los datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento.*

***Artículo 26.*** *El responsable deberá informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto.*

*Por regla general, el aviso de privacidad deberá ser difundido por los medios electrónicos y físicos con que cuente el responsable.*

*Para que el aviso de privacidad cumpla de manera eficiente con su función de informar, deberá estar redactado y estructurado de manera clara y sencilla.*

*Cuando resulte imposible dar a conocer al titular el aviso de privacidad, de manera directa o ello exija esfuerzos desproporcionados, el responsable podrá instrumentar medidas compensatorias de comunicación masiva de acuerdo con los criterios que para tal efecto emita el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.*

***Artículo 27.*** *El aviso de privacidad a que se refiere el artículo 3, fracción II, se pondrá a disposición del titular en dos modalidades: simplificado e integral. El aviso simplificado deberá contener la siguiente información:*

*I. La denominación del responsable;*

*II. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieran el consentimiento del titular;*

*III. Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar:*

*a) Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales, y*

*b) Las finalidades de estas transferencias;*

*IV. Los mecanismos y medios disponibles para que el titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren el consentimiento del titular, y*

*V. El sitio donde se podrá consultar el aviso de privacidad integral.*

*La puesta a disposición del aviso de privacidad al que refiere este artículo no exime al responsable de su obligación de proveer los mecanismos para que el*

*titular pueda conocer el contenido del aviso de privacidad al que se refiere el artículo siguiente.*

*Los mecanismos y medios a los que se refiere la fracción IV de este artículo, deberán estar disponibles para que el titular pueda manifestar su negativa al tratamiento de sus datos personales para las finalidades o transferencias que requieran el consentimiento del titular, previo a que ocurra dicho tratamiento.*

***Artículo 28.*** *El aviso de privacidad integral, además de lo dispuesto en las fracciones del artículo anterior, al que refiere la fracción V del artículo anterior deberá contener, al menos, la siguiente información:*

*I. El domicilio del responsable;*

*II. Los datos personales que serán sometidos a tratamiento, identificando aquéllos que son sensibles;*

*III. El fundamento legal que faculta al responsable para llevar a cabo el tratamiento;*

*IV. Las finalidades del tratamiento para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieren el consentimiento del titular;*

*V. Los mecanismos, medios y procedimientos disponibles para ejercer los derechos ARCO;*

*VI. El domicilio de la Unidad de Transparencia, y*

*VII. Los medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.*

***Artículo 29.*** *El responsable deberá implementar los mecanismos previstos en el artículo 30 de la presente Ley para acreditar el cumplimiento de los principios, deberes y obligaciones establecidos en la presente Ley y rendir cuentas sobre el tratamiento de datos personales en su posesión al titular e Instituto o a los Organismos garantes, según corresponda, caso en el cual deberá observar la Constitución y los Tratados Internacionales en los que el Estado mexicano sea parte; en lo que no se contraponga con la normativa mexicana podrá valerse de estándares o mejores prácticas nacionales o internacionales para tales fines.*

***Artículo 30.*** *Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en la presente Ley están, al menos, los siguientes:*

*I. Destinar recursos autorizados para tal fin para la instrumentación de programas y políticas de protección de datos personales;*

*II. Elaborar políticas y programas de protección de datos personales, obligatorios y exigibles al interior de la organización del responsable;*

*III. Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones y demás deberes en materia de protección de datos personales;*

*IV. Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran;*

*V. Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales;*

*VI. Establecer procedimientos para recibir y responder dudas y quejas de los titulares;*

*VII. Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la presente Ley y las demás que resulten aplicables en la materia, y*

*VIII. Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la presente Ley y las demás que resulten aplicables en la materia.*

## COMENTARIO

**Nelson Remolina Angarita**

### I. Antecedentes

El tratamiento[17] de datos personales y el uso de bases de datos son actividades cotidianas e importantes para el Estado, las empresas y los particulares que requieren dicha información para tomar e implementar decisiones de diversa naturaleza (económica, seguridad nacional, social, política, laboral, impuestos, estadísticas, profesional, académica, financiera, comercial, etc.). Igualmente, los datos personales representan, en algunos casos, el principal activo de empresas que se dedican a venderlos, alquilarlos y cederlos. En otros casos,

[17] A efectos del presente documento, las expresiones "tratar" o "tratamiento" se entenderán como cualquier operación o conjunto de operaciones aplicadas a datos personales, como la recolección, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción.

se utilizan para tomar decisiones sobre las personas o para fijar políticas públicas, económicas, de riesgo, de marketing, entre otras.

Las Tecnologías de la Información y la Comunicación (TIC) no sólo son consideradas como el "símbolo emblemático de la cultura contemporánea"[18] sino que han contribuido a la *datatificación* de la sociedad actual y a la consolidación del dato personal como el bien más apetecido de la economía digital.

El tratamiento de datos personales es uno de los temas que en los últimos cincuenta años ha llamado la atención de los reguladores y las organizaciones. Inicialmente fue poco reglamentado, pero en esta última década estamos presenciando una eclosión mundial de normas sectoriales y generales, una revisión de las primeras iniciativas regulatorias así como múltiples conferencias a todo nivel que ponen de presente la indiscutible relevancia social y económica del tratamiento de la información de las personas.

El derecho a la protección de datos personales que conocemos en el año 2018 ha tenido cambios desde sus primeras manifestaciones regulatorias de la década de los setenta y en los documentos emitidos posteriormente. A los motivos iniciales que dieron origen a su reglamentación se sumaron otros factores que han hecho que los retos de la protección de este derecho sean diferentes a los inicialmente previstos.

El derecho al debido tratamiento de los datos personales parte del supuesto de que la recolección y uso de los datos no es algo que sólo le interesa al titular del dato porque reconoce que los datos son necesarios para realizar muchas actividades lícitas, legítimas y de interés general o particular, según el caso. Por eso no es un derecho para oponerse al tratamiento, sino para exigir un correcto tratamiento de la información sobre las personas. No se opone al uso informático sino al abuso informático.

Varios países cuentan con regulaciones generales y sectoriales así como jurisprudencia sobre tratamiento de datos personales. Aunque se ha procurado armonizar internacionalmente los principales aspectos sobre el tratamiento de datos personales, en la práctica cada Estado cuenta con normas que, parcialmente, siguen dichos documentos internacionales, pero que al mismo tiempo están impregnadas de las particularidades sociales, políticas, culturales y jurídicas de cada uno. Adicionalmente, cada sistema jurídico nacional cuenta con diversas herramientas jurídicas (constitucionales, administrativas, judiciales, entre otras) para proteger el derecho al debido tratamiento de datos personales.

[18] García, A. (2007). La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado, *Boletín Mexicano de Derecho Comparado*, Universidad Nacional Autónoma de México, nueva serie, año XL, núm. 120, septiembre-diciembre, p. 744.

A principios de 2017, en los Estados Unidos Mexicanos se expidió la LGPDPPSO, mediante la cual, entre otros, se incorpora en el Capítulo I del Título Segundo un conjunto de principios que el responsable del tratamiento debe cumplir cuando recolecta, almacena, usa, circula o realiza cualquier actividad con datos personales, a saber: principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales. Este capítulo tiene como propósito referirnos, de manera general, a la importancia de los principios para proteger los derechos de las personas y la labor de armonización internacional que precedió a la incorporación de los mismos en la citada ley.

Nos referiremos brevemente a los principales aspectos de cada principio con especial referencia al de consentimiento y responsabilidad. En este sentido nuestros comentarios son una introducción a cada tema pero no un desarrollo meticuloso de cada principio.

## II. Relevancia temática y contexto

**1. Relevancia de los principios en el tratamiento de datos personales.** Como es sabido, el principal objetivo del derecho a la protección de los datos personales es el respeto de los derechos de las personas cuando sus datos son tratados por terceros. ¿Cómo lograr lo anterior?: exigiendo a los terceros un debido tratamiento de los datos personales. Recuérdese que "la protección de las personas respecto al tratamiento automatizado de datos de carácter personal"[19] hace parte del más antiguo y único instrumento jurídico internacional vinculante y ratificado por 46 países. Nótese que el Convenio 108 de 1981 no tiene como objeto proteger los datos sino "garantizar, […], a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales […] con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona".[20]

Las regulaciones sobre tratamiento de datos personales no sólo confieren una serie de facultades a los titulares de los datos (conocer, actualizar, corregir, eliminar, entre otras) sino que se enfocan en exigir a quienes los poseen o administran (responsables, encargados o usuarios en general) una serie de requisitos y obligaciones dentro de las cuales se encuentra el deber de observar los principios sobre el tratamiento de datos personales. El desconocimiento de dichos principios implica, además de una infracción a la ley, una vulneración del debido proceso en el tratamiento de los datos.

---

[19] Cfr. Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal.

[20] *Ibíd*., artículo 1. Ese mismo objetivo se replicó en el numeral primero del artículo 1 de la Directiva 95/46/CE según el cual "los Estados miembros garantizarán, […], la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales".

Es necesario que el tratamiento sea debido (como sucede con el debido proceso), es decir, correcto o realizado conforme a la ley, respetando los principios de la misma, entre otros. No puede ser cualquier tipo de tratamiento sino que debe ser correcto, ajustado a la ley y respetuoso de los derechos de las personas y de los principios establecidos para dicho efecto.

Así las cosas, en nuestra opinión, los principios cumplen varios objetivos entre los que se encuentran los siguientes:

1. Son un instrumento para garantizar el debido tratamiento de los datos personales y, por ende, el respeto de los derechos de los titulares de los datos.

2. Representan un límite al tratamiento de los datos personales en el sentido que no puede hacerse de cualquier manera sino de forma respetuosa de unos mínimos que son, precisamente, los principios.

3. Constituyen una herramienta de interpretación de la ley y de aplicación correcta de la misma, así como el factor determinante de la solución de casos concretos que se sometan a consideración de las autoridades o los jueces.

En efecto, para Ciro Angarita Barón "los principios son normas que establecen un deber ser específico […] y […] tienen una mayor eficacia y, por lo tanto, una mayor capacidad para ser aplicados de manera directa e inmediata".[21] Pese a las diversas acepciones sobre el significado de *principios*,[22] no debe perderse de vista que ellos recogen las ideas fundamentales que inspiran el derecho de la protección de datos. Como lo mencioné en otra ocasión, los principios "no son meras enunciaciones teóricas o elucubraciones retóricas sin uso práctico. Se trata de una serie de reglas materiales concebidas para desarrollar y asegurar la consecución de los fines de las normas sobre el tratamiento de datos. Estos principios tienen fuerza vinculante, aplicación práctica y son los que definen si un tratamiento de datos se está o no realizando de manera leal, lícita, transparente y adecuada".[23]

Los principios son las reglas fundamentales de aplicación obligatoria para garantizar el respeto de las personas cuando sus datos recolectados, almacenados, usados o circulados han sido objeto de cualquier actividad por parte de responsables o encargados del tratamiento. Por eso, señala la jurisprudencia que "los principios […] consagran prescripciones jurídicas generales que suponen una delimitación política y axiológica reconocida y, en

[21] Cfr. República de Colombia. Corte Constitucional, sentencia T-406 de 1992. Magistrado Ciro Angarita Barón.
[22] Consúltese las múltiples definiciones de este término en el *Diccionario de la lengua española*.
[23] Cfr. Remolina, N. (2013). *Tratamiento de datos personales: aproximación internacional y comentarios a la ley 1581 de 2012*. Bogotá: Legis editores, p. 177.

consecuencia, restringen el espacio de interpretación, lo cual hace de ellos normas de aplicación inmediata […]. Su alcance normativo no consiste en la enunciación de ideales que deben guiar los destinos institucionales y sociales con el objeto de que algún día se llegue a ellos; […]. Los principios expresan normas jurídicas para el presente; son el inicio del nuevo orden".[24]

En otras palabras, los principios son el camino para garantizar la protección efectiva de los derechos de las personas cuando sus datos son tratados por terceros.

Los principios también pueden verse como los límites al tratamiento de los datos personales, porque los responsables o encargados no pueden tratar esa información de cualquier manera sino de forma respetuosa de la ley y, por ende, los principios de la misma. Refiriéndose al rol de los principios la jurisprudencia ha establecido que los mismos definen "el contexto axiológico dentro del cual debe moverse el proceso informático. Según este marco general, existen unos parámetros generales que deben ser respetados para poder afirmar que el proceso de acopio, uso y difusión de datos personales sea constitucionalmente legítimo".[25]

Los principios no sólo son herramientas de uso obligatorio y referencia en el desarrollo o reglamentación de la ley sino que deben tenerse presentes para la interpretación y aplicación de la misma. En todos los casos la ley se debe aplicar de manera armónica e integral conforme a los lineamientos que emergen de los principios. En línea con lo anterior, la jurisprudencia ha señalado que "los principios […] son una pauta de interpretación ineludible […] y están dotados de toda la fuerza […]. Sin embargo, no siempre son suficientes por sí solos para determinar la solución necesaria en un caso concreto".[26]

**2. Armonización internacional sobre los principios para el tratamiento de datos personales.** Las respuestas normativas al tratamiento de datos personales se caracterizan, entre otras cosas, por tener enfoque internacional y ser armonizadas. Por eso, la recolección, almacenamiento, uso, circulación y demás actividades sobre los datos personales han sido objeto de una labor de armonización internacional regulatoria con miras a lograr un consenso jurídico coherente sobre temas cardinales de dicha materia.[27] En ese sentido, diferentes organizaciones internacionales, redes especializadas o grupos de autoridades han publicado documentos contentivos de las reglas que deben observarse

[24] Cfr. República de Colombia. Corte Constitucional, sentencia T-406 de 1992. Magistrado Ciro Angarita Barón.

[25] Cfr. República de Colombia. Corte Constitucional, sentencia C-748 de 2011, numeral 2.6.3.

[26] Cfr. República de Colombia. Corte Constitucional, sentencia C-748 de 2011, numeral 2.6.3.

[27] En la Declaración Conjunta entre la Unión Europea y Estados Unidos sobre Comercio Electrónico de 1997 se puntualizó que "el papel de los gobiernos es proporcionar un marco legal claro y consistente, promover un entorno competitivo en el que el comercio electrónico pueda florecer y asegurar la protección adecuada de objetivos de interés público como la intimidad, los derechos de propiedad intelectual, la prevención del fraude, la protección del consumidor y la seguridad nacional".

en el tratamiento de datos personales, dentro de las cuales se encuentran varios principios que evocan los grandes mensajes o propósitos que se deben materializar para lograr que los derechos de las personas no sean amenazados o vulnerados por la indebida recolección, almacenamiento, uso o circulación de dicha información.

En la siguiente tabla resumimos los principales documentos emitidos por diferentes organizaciones. Para el efecto enunciaremos los textos proferidos más recientemente:

**Tabla 1. Principales documentos internacionales sobre tratamiento de datos personales**

| Organización | Principales documentos |
|---|---|
| RIPD | Estándares de Protección de Datos Personales para los Estados Iberoamericanos (2017). |
| UE | 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).<br>Protocolo adicional al convenio 108 del Consejo para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal y relativo a la transferencia de datos (2001).<br>Carta de los derechos fundamentales de la Unión Europea (2000).<br>Convenio 108 del Consejo para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal (1981). |
| OEA | Principios de la OEA sobre la privacidad y la protección de datos personales con anotaciones (2015).[28] |
| OCDE | Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales (2013, 1980). |
| CIAPDP | Estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal –Resolución de Madrid– (2009). |
| APEC | Marco de privacidad APEC (2004). |
| ONU | Principios rectores para la reglamentación de los ficheros computadorizados de datos personales (1990).[29] |

Fuente: Elaboración del autor.

[28] Cfr. Organización de los Estados Americanos. (2015). *86º Período Ordinario de Sesiones*, 23-27 de marzo. Río de Janeiro, Brasil, OEA/Ser.Q CJI/doc. 474/15 rev.2 26 marzo 2015.

[29] Asamblea General de las Naciones Unidas. (1990). *Resolución 45/95 de 14 de diciembre*.

Esos documentos son fruto de una labor de armonización de los aspectos centrales del tratamiento de datos personales. Procuran asegurar unos mínimos en las actividades que impliquen la recolección, almacenamiento y uso de dicha información, estableciendo unos principios sobre la materia e imponiendo, en ciertos casos, criterios de comportamiento razonable. Dado su origen extranjero reflejan conceptos, instituciones y finalidades de otras culturas y sistemas jurídicos que, según el país, pueden coincidir o ser consistentes con las tradiciones jurídicas locales. Muchos de ellos han sido el modelo o guía de normas locales y un referente para interpretar o suplir vacíos de las mismas.

El análisis de estos documentos internacionales es necesario por varias razones: a) muestran que la protección de datos personales no es nueva y que su origen no es una creación original del legislador local, sino fruto de una tendencia internacional para tratar de conciliar las necesidades de los negocios internacionales y el respeto de algunos derechos humanos; b) permiten determinar el origen y alcance de muchos términos, definiciones e instituciones utilizados en las regulaciones locales; c) proporcionan una idea de las tendencias de ciertos aspectos afines al tratamiento de datos personales y permiten tener una aproximación general a los principios e instituciones existentes en otras partes del mundo.

No obstante lo anterior, es necesario tener presente lo siguiente respecto de los documentos internacionales: a) las expresiones y alcances que le confieren a ciertos principios e instituciones no coinciden, necesariamente, con los términos de las regulaciones locales; b) no todos los documentos mencionan los mismos temas. Por ejemplo, la mayoría se refieren al principio de seguridad y a las reglas sobre transferencias internacionales, pero no todos definen que es un dato personal, la autorización o el consentimiento; c) en algunos casos y para ciertas cuestiones los términos utilizados son muy amplios, poco claros y redactados en términos “gaseosos” que dificultan tener certeza objetiva de lo que se quiere o no se quiere. Adicionalmente, las versiones originales de algunos documentos no fueron escritas en castellano y no existen, en todos los casos, versiones oficiales en dicho idioma. Finalmente, todas las organizaciones parten del supuesto de respetar derechos humanos pero la misión principal o razón de ser de algunas entidades son el crecimiento económico (APEC),[30] el bienestar económico y social (OCDE),[31] lo cual explica

[30] APEC es el Foro de Cooperación Económica de Asia-Pacífico y su principal objetivo es apoyar el crecimiento económico sostenible y la prosperidad en la región. Procuran defender el comercio y la inversión, promover y acelerar la integración económica regional, fomentar la cooperación económica y técnica, mejorar la seguridad humana y facilitar un ambiente de negocios favorable y sostenible. Disponible en: http://www.apec.org/About-Us/About-APEC/Mission-Statement.aspx. Más información sobre APEC en: http://www.apec.org/

[31] La misión de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) es promover políticas que mejoren el bienestar económico y social de las personas en todo el mundo. Es un foro en el que los gobiernos pueden trabajar juntos para compartir experiencias y buscar soluciones a problemas comunes e impulsar cambios económicos, sociales y medioambientales. Disponible en:

por qué en ciertos documentos se incluyen o excluyen algunas cuestiones o se hace énfasis en unas cosas y se dejan de lado otras.

Los documentos internacionales tienen origen en varias partes del mundo —Europa, Norteamérica, Latinoamérica— con dispares tradiciones jurídicas. Así las cosas, su interpretación y alcance deben considerar las diversas culturas jurídicas que están inmersas en cada texto. En otras palabras, los textos establecen reglas generales aplicables al tratamiento de datos personales, pero fueron redactados en países con disímiles tradiciones jurídicas, condiciones económicas y políticas. Reflejan algunos conceptos que se encuentran en varios sistemas jurídicos pero no reemplazan dichos sistemas ni borran absolutamente las normas, culturas y tradiciones jurídicas locales. Procuran armonizar mínimos para el tratamiento global de datos personales pero no unifican dichas reglas. Pese a lo anterior, recalcamos, no dejan de ser muy importantes y por ello haremos, cuando sea pertinente, las necesarias referencias a tales aspectos.

## III. Análisis del contenido

**1. Los principios de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados frente al escenario internacional.** Como mencionamos, la LGPDPPSO incorporó los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales. Estos principios son consistentes con los que internacionalmente se han desarrollado durante varias décadas.

En la tabla 2 destacamos cronológicamente algunas cuestiones relevantes sobre los documentos más emblemáticos que han emitido entidades internacionales sobre tratamiento de datos personales con miras a validar que la LGPDPPSO incorporó la mayoría de ellos en su articulado.

http://www.oecd.org/about/. Más información sobre la OCDE en: http://www.oecd.org/.

**Tabla 2. Principios sobre tratamiento de datos personales incorporados en documentos internacionales**

| Principio / Organización | RIPD 2017 | UE 2016 | OEA 2015 | OCDE 2013 | CIAPDP 2009 | APEC 2004 | ONU 1990 |
|---|---|---|---|---|---|---|---|
| Legitimación | * | * | * | * | * | * | X |
| Licitud | * | * | * | * | * | * | * |
| Lealtad | * | * | * | | * | | * |
| Transparencia / Apertura /Aviso | * | * | * | * | * | * | X |
| Finalidad / Limitación de la finalidad / Uso limitado | * | * | * | * | * | * | * |
| Proporcionalidad / Pertinencia / Minimización de datos | * | * | * | * | * | * | X |
| Calidad / Exactitud | * | * | * | * | * | * | * |
| Responsabilidad | * | * | * | * | * | * | X |
| Seguridad | * | * | * | * | * | * | * |
| Confidencialidad | * | * | * | X | * | X | X |
| Limitación del plazo de conservación / Retención | X | * | * | X | X | X | * |
| Prevención del daño | X | X | X | X | X | * | X |
| Elección | X | X | X | X | X | * | X |
| No discriminación | X | X | X | X | X | X | * |

Fuente: Elaboración del autor.

Como se observa, la LGPDPPSO incluye los anteriores principios salvo algunos desarrollados por la ONU (principio de no discriminación) y APEC (prevención del daño y elección). No obstante, los principios de dicha ley son adecuados para garantizar un debido tratamiento de los datos personales.

A continuación nos referiremos a cada principio pero haremos especial referencia a los principios del consentimiento y de responsabilidad.

Como lo mencionamos, el Capítulo I del Título Segundo de la ley enuncia un conjunto de principios que el responsable del tratamiento debe cumplir cuando recolecta, almacena, usa, circula o realiza cualquier actividad con datos personales. Los siguientes son los principales aspectos de dichos preceptos.

**1) Principio de licitud.** Este principio (artículo 17) exige a los responsables que el tratamiento de los datos personales lo realicen observando lo que ordena la ley. De esta forma se busca que el tratamiento de datos personales no se efectúe de manera caprichosa o arbitraria sino de forma objetiva y respetando el Estado de derecho, el cual es un elemento esencial de la democracia. Este principio pone de manifiesto que el tratamiento de datos es una actividad con facultades o atribuciones limitadas o definidas en la ley. Por lo tanto, no puede hacerse de cualquier forma sino de la manera que lo indica.

**2) Principio de finalidad.** Este principio (artículo 18) busca que el tratamiento tenga como objetivo la realización de "finalidades concretas, lícitas, explícitas y legítimas, relacionadas con las atribuciones que la normatividad aplicable les confiera". Así, quien trate datos no puede usar los mismos para cualquier propósito sino para aquellos establecidos en el aviso de privacidad, salvo que "cuente con atribuciones conferidas en la ley y medie el consentimiento del titular", situación en la cual excepcionalmente podrá tratar los datos para otras finalidades. En suma, el principio de finalidad busca evitar que se recolecten datos para hacer con ellos lo que sea y delimita los usos que pueda darle el responsable.

**3) Principio de proporcionalidad.** En línea con lo anterior, el artículo 25, ordena que sólo se pueden tratar los "datos personales que resulten adecuados, relevantes y estrictamente necesarios para la finalidad que justifica su tratamiento". En otras palabras, el tratamiento de datos personales sólo deberá circunscribirse a los que resulten adecuados, relevantes y no excesivos en relación con la finalidad del tratamiento. Por lo tanto, no está permitido recolectar o usar datos que no guarden estrecha relación con la finalidad del tratamiento.

**4) Principio de lealtad.** Con este principio se proscribe el tratamiento tramposo, desleal al titular, deshonesto, pícaro y no ético de la información sobre las personas. Por eso, el artículo 19 ordena que "el responsable no deberá obtener y tratar datos personales, a través de medios engañosos o fraudulentos, privilegiando la protección de los intereses del titular y la expectativa razonable de privacidad". Nótese que los derechos del titular dependen, principalmente, de lo que haga o deje de hacer el responsable. Al titular le es imposible controlar lo que él hace con su información. Por eso, al titular no le queda más remedio que confiar en la buena fe, diligencia y ética del responsable. Así las cosas, la ley prohíbe al responsable defraudar esa confianza y recurrir a mecanismos oscuros, ilegales o poco transparentes para recolectar y tratar los datos. La lealtad significa, entre otras, tratar los datos sin engaño y de la forma como lo hemos prometido o anunciado, incluso en circunstancias adversas. El principio de lealtad no se cumple cuando, por ejemplo, traicionamos la confianza que nos ha depositado el titular del dato.

**5) Principio del consentimiento.** La ley define el consentimiento 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 2), precisa que éste será libre, cuando no "medie error, mala fe, violencia o dolo que puedan afectar la manifestación de voluntad del titular", específico, cuando las finalidades sean "concretas, lícitas, explícitas y legítimas que justifiquen el tratamiento" e informado, cuando el "titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales" (artículo 20). Adicionalmente, ordena que el consentimiento puede ser expreso o tácito, indicando que es tácito "cuando habiéndose puesto a disposición del titular el aviso de privacidad, éste no manifieste su voluntad en sentido contrario" (artículo 21). El concepto, la obligatoriedad del uso de los avisos de privacidad y su contenido fueron regulados principalmente en los artículos 3, 26-28 de la ley. Es positivo que el consentimiento de la persona siga siendo un elemento legitimador del tratamiento de datos, pero es importante destacar que no es un mecanismo de protección del titular, sino una forma de reconocer que el ser humano es quien decide, por regla general, a quién entrega sus datos, para qué propósitos y a quién se puede dar acceso para hacerlos circular. El consentimiento reconoce que la persona es el titular del dato y, por ende, ella es quien, en principio, tiene control sobre su información y algunos aspectos de su vida relacionados con su información. Existe una campaña de extinción del consentimiento argumentando que no sirve para nada o que es una barrera para el desarrollo de algunas actividades o porque afecta el modelo de negocios de algunas empresas. Aunque en la práctica el consentimiento tiene un efecto simbólico, no por ello deja de ser muy importante en las relaciones humanas. Eliminar el consentimiento sería tanto como permitir que cualquier persona ingrese a nuestra casa sin nuestra autorización, o que el día del matrimonio no se les pregunte a las personas si desean casarse. ¿El hecho de que una empresa actúe de manera profesional, diligente y ética justifica que la misma no obtenga nuestra autorización para tratar nuestros datos personales? ¿Si una persona es "perfecta" o por lo menos la esposa o el esposo "ideal" nos debemos casar con ella sin que nos consulten cuál es nuestra voluntad?

**6) Principio de calidad.** El artículo 23 exige que los datos personales sean veraces, exactos, completos, correctos y actualizados. Le corresponde al responsable adoptar medidas para que ello sea así. En suma, la información de calidad es una condición para el debido tratamiento de los datos y de ella dependen algunos derechos de las personas como su buen nombre o que las decisiones que se adopten con fundamento en los datos personales sean correctas, pertinentes o apropiadas. No debe perderse de vista que la información es, por excelencia, una herramienta para tomar decisiones. Si no se logra mantener sistemas de información de calidad, las organizaciones deben reflexionar si en su posesión tienen "bases de datos o basureros de datos". La redacción del principio da un espacio importante a la vigencia del

dato de manera que se deje de tratar información que ya no es necesaria para cumplir con las finalidades previstas en el aviso de privacidad. En estos casos, los datos "deberán ser suprimidos, previo bloqueo en su caso, y una vez que concluya el plazo de conservación de los mismos". Estos plazos de conservación están vinculados a la finalidad del tratamiento de las exigencias legales. En ese sentido, la parte final del artículo 23 señala que "los plazos de conservación de los datos personales no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron su tratamiento, y deberán atender a las disposiciones aplicables en la materia de que se trate y considerar los aspectos administrativos, contables, fiscales, jurídicos e históricos de los datos personales". Para cumplir lo anterior, el artículo 24 ordena al responsable "establecer y documentar los procedimientos para la conservación y, en su caso, bloqueo y supresión de los datos personales que lleve a cabo". En estos casos, continúa la norma, "el responsable deberá incluir mecanismos que le permitan cumplir con los plazos fijados para la supresión de los datos personales, así como para realizar una revisión periódica sobre la necesidad de conservar los datos personales". En suma, los datos personales no se deben tratar indefinidamente sino sólo por el período de tiempo necesario para cumplir la finalidad para la cual fueron recolectados.

**7) Principio de información.** Con este principio se busca que el titular tenga conocimiento de los principales aspectos que regirán el tratamiento de sus datos personales. En ese sentido, el artículo 26 ordena al responsable "informar al titular, a través del aviso de privacidad, la existencia y características principales del tratamiento al que serán sometidos sus datos personales, a fin de que pueda tomar decisiones informadas al respecto". El aviso de privacidad, como se observa, se constituye en el mecanismo para informar al titular los aspectos indicados. Por eso, la norma es enfática en exigir que dichos avisos cumplan algunos requerimientos como los siguientes: (1) estar redactados y estructurados de manera clara y sencilla para que puedan ser entendidos por el titular; (2) contener cierta información indicada en los artículos 27 y 28 según se trate del aviso de privacidad simplificado o integral, respectivamente; (3) ser difundido por los medios electrónicos o físicos con que cuente el responsable.

**8) Principio de responsabilidad.** El reto de la ley es el cumplimiento real y efectivo de la misma. Por eso, los artículos 29 y 30 de la ley envían un mensaje contundente a los sujetos obligados ordenándoles que adopten medidas de buen gobierno corporativo de datos que garanticen que los principios de la ley y sus demás disposiciones se cumplan en la práctica y no, como a veces sucede, se conviertan en "letra muerta". El principio de responsabilidad (*accountability*) está incorporado en la mayoría de los documentos internacionales referenciados en la tabla 2. Esto no es novedoso en el contexto iberoamericano ya que fue analizado en el año 2006 por la RIPD. En aquel entonces se expidió un documento sobre autorregulación y

protección de datos que guarda cercana relación con el principio en comento en la medida que la materialización del mismo depende, en gran parte, de lo que internamente decidan hacer las organizaciones. En otras palabras, dicho principio se engloba dentro del concepto de autorregulación y desde esa perspectiva es importante tener presente lo que plantea la RIPD: En primer lugar, la "autorregulación sólo redundará en beneficio real de las personas en la medida que sea **bien concebida, aplicada y cuente con mecanismos que garanticen su cumplimiento de manera que no se constituyan en meras declaraciones simbólicas de buenas intenciones** sin que produzcan efectos concretos en la persona cuyos derechos y libertades pueden ser lesionados o amenazados por el tratamiento indebido de sus datos personales"; en segundo lugar, recalca la RIPD que es "imprescindible que los instrumentos de autorregulación **estén acompañados de herramientas que los hagan eficaces**"; finalmente, insiste en que "las medidas de autorregulación deben **evaluarse desde dos perspectivas concomitantes: la objetiva y la funcional [...]. La segunda, por su parte, busca establecer el nivel de efectividad práctica de dichas normas**". Un análisis de los anteriores factores permitirá determinar el verdadero grado de contribución de los instrumentos de autorregulación a la protección de los datos personales. Por eso, la RIPD considera "oportuno que **se prevean fórmulas para evaluar periódicamente la eficacia de los instrumentos** de autorregulación, midiendo el grado de satisfacción de los afectados y, en su caso, actualizando el contenido para adaptarlo a la normativa general o sectorial de protección de datos existente en cada momento".[32] Dicho principio fue incluido en la Resolución de Madrid de 2009 en donde se exige a los responsables y encargados del tratamiento adoptar medidas apropiadas para cumplir sus obligaciones legales y estar en capacidad de evidenciar el correcto cumplimiento de sus deberes. Para tal efecto deben contar con mecanismos idóneos que les permitan probar lo anterior ante las autoridades y los titulares de los datos. La OCDE, por su parte, incorporó el *accountability principle* en sus directrices de 1980 estableciendo que el responsable del tratamiento tiene el deber de adoptar las medidas necesarias para cumplirlas efectivamente. En 2013 se revivió con fuerza y pautas concretas el principio de responsabilidad con ocasión de la revisión de los principios de la OCDE. Dentro de las novedades del OECD *privacy framework* de 2013 se incluye la creación de los programas de gestión de privacidad (*Privacy management programmes*) como el mecanismo operativo a través del cual las organizaciones implementan la protección de la privacidad y el tratamiento de los datos personales. Allí se establecen, en la parte tres, los deberes a cargo de los responsables del tratamiento para

[32] Texto resaltado por el autor. Cfr. Red Iberoamericana de Protección de Datos, Grupo de trabajo temporal sobre autorregulación y protección de datos personales. (2006). Documento adoptado durante las sesiones de trabajo del 3 al 5 de mayo en la ciudad de Santa Cruz (Bolivia). Disponible en: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/RIPD-AUTORREGULACIÓN-Y-PROTECCIÓN-DE-DATOS-PERSONALES-BOLIVIA-2006.pdf

implementar adecuadamente el *accountability principle*. Los programas de gestión de datos (*privacy management program*) son la herramienta para lograr un buen gobierno corporativo en el tratamiento de datos personales que redunde en beneficio de los derechos de las personas y de los sujetos obligados, porque les permite maximizar el uso de la información para cumplir sus cometidos constitucionales y legales. Más recientemente, el RGPD de 2016 incluyó la responsabilidad como un principio relativo al tratamiento[33] y la RIPD desarrolló mecanismos[34] concretos para cumplir con el principio en comento, los cuales fueron incorporados a los Estándares de Protección de Datos para los Estados Iberoamericanos,[35] aprobados en junio de 2017 en el XV Encuentro Iberoamericano de Protección de Datos, celebrado en Santiago de Chile. El principio de responsabilidad demanda menos retórica y más acción en el cumplimiento de los deberes que imponen las regulaciones sobre tratamiento de datos personales. El éxito del mismo dependerá del compromiso real de los directivos de los sujetos obligados ya que sin su apoyo franco y decidido todo esfuerzo será insuficiente para diseñar, implementar, revisar, actualizar y evaluar los programas de gestión de datos. Es necesario destinar recursos (económicos y humanos) para esta labor y poner a trabajar armónicamente varias dependencias de la organización ya que esto no es sólo un tema jurídico sino ante todo una cuestión de gestión gerencial y

[33] El numeral 2 del artículo 5 sobre los principios relativos al tratamiento dice lo siguiente: "El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo 'responsabilidad proactiva' y el artículo 24 —Responsabilidad del responsable del tratamiento— ordena que: 1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario; 2. Cuando sean proporcionadas en relación las actividades del tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos; 3. La adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento".

[34] Los numerales 20.3 y 20.4 de los Estándares de Protección de Datos para los Estados Iberoamericanos dicen: "20.3 Entre los mecanismos que el responsable podrá adoptar para cumplir con el principio de responsabilidad se encuentran, de manera enunciativa mas no limitativa, los siguientes: a) Destinar recursos para la instrumentación de programas y políticas de protección de datos personales; b) Implementar sistemas de administración de riesgos asociados al tratamiento de datos personales; c) Elaborar políticas y programas de protección de datos personales obligatorios y exigibles al interior de la organización del responsable; d) Poner en práctica un programa de capacitación y actualización del personal sobre las obligaciones en materia de protección de datos personales; e) Revisar periódicamente las políticas y programas de seguridad de datos personales para determinar las modificaciones que se requieran; f) Establecer un sistema de supervisión y vigilancia interna y/o externa, incluyendo auditorías, para comprobar el cumplimiento de las políticas de protección de datos personales; g) Establecer procedimientos para recibir y responder dudas y quejas de los titulares. 20.4. El responsable revisará y evaluará permanentemente los mecanismos que para tal efecto adopte voluntariamente para cumplir con el principio de responsabilidad, con el objeto de medir su nivel de eficacia en cuanto al cumplimiento de la legislación nacional aplicable".

[35] El texto oficial de los Estándares puede consultarse en la página web de la Red Iberoamericana de Protección de Datos: http://www.redipd.es/documentacion/common/Estandares_Esp_Con_logo_RIPD.pdf

estratégica de gobierno corporativo. El reto de los sujetos obligados frente al principio de responsabilidad va mucho más allá de la mera expedición de documentos porque exige que se demuestre el cumplimiento real y efectivo en la práctica cuando realizan sus funciones. Con este principio se quiere que los mandamientos constitucionales y legales sobre tratamiento de datos personales sean una realidad verificable y redunden en beneficio de la protección de los derechos de las personas. La LGPDPPSO indica en el artículo 30 las acciones básicas que el sujeto obligado debe adelantar para implementar el principio de responsabilidad, ordenándoles que (a) destinen recursos para cumplir los programas de gestión de datos; (b) elaboren políticas y programas de protección de datos de carácter obligatorio al interior de cada sujeto obligado; (c) capaciten permanentemente a los funcionarios para consolidar una cultura de tratamiento responsable de datos personales; (d) revisen periódicamente las medidas de seguridad; (e) implementen procesos de control interno y externo respecto de las políticas y los programas de protección de datos; (f) habiliten herramientas e implementen procesos para atención de consultas y reclamos de los titulares; (g) desarrollen el principio de protección de datos desde el diseño y por defecto en todas las gestiones o procesos que realice el sujeto obligado y que implique tratamiento de datos personales.

Particular importancia debe darse a las acciones preventivas en materia de tratamiento de datos, razón por la cual son cruciales las medidas tendentes a: (a) inculcar y consolidar en el equipo humano de los sujetos obligados una cultura de debido tratamiento de datos personales, pues poco se logra si los servidores públicos no son conscientes de la importancia del derecho de la protección de datos, ni saben que si tratan indebidamente los datos personales afectan los derechos humanos de las personas; (b) promover el diseño de procesos y desarrollo de tecnologías que desde el principio tengan presente el debido tratamiento de datos como un factor relevante. En suma, se trata de implementar la “protección de datos desde el diseño y por defecto” con miras a que desde antes que se recolecte información y durante todo el ciclo de vida de la misma, se adopten procedimientos y medidas preventivas de diversa naturaleza —tecnológica, organizacional, humana— para evitar vulneraciones al derecho a la protección de datos personales, así como fallas de seguridad o indebidos tratamientos de datos personales.

La privacidad y la seguridad deben ser parte del diseño, arquitectura y configuración predeterminada de cualquier procedimiento de gestión de información. Se deben utilizar mecanismos y diseñar procedimientos para que por defecto, sólo sean objeto de tratamiento los datos estrictamente necesarios para cumplir una finalidad específica y para que los datos personales no sean accesibles a un número indeterminado de personas.

Ann Cavoukian señala, con razón, que “todos podemos estar seguros de una cosa – ¡Lo predeterminado es lo que manda!”. Por eso, los sujetos obligados deben revisar los procesos actuales y diseñar los futuros de manera que el debido tratamiento de datos personales esté incrustado como configuración predeterminada para que, en palabras de la citada autora, “los datos personales estén protegidos automáticamente en cualquier sistema” o proceso. Si pensamos en el debido tratamiento de datos desde el principio —y no al final cuando todo se ha hecho— garantizaremos mejores niveles de adecuado tratamiento de la información de las personas.

## IV. Conclusiones

Internacionalmente se ha identificado un grupo de postulados generales contentivos de las directrices centrales que inspiran el debido tratamiento de los datos personales. Estos principios son una serie de reglas concebidas para procurar que la recolección y uso de la información personal no afecte o lesione los derechos de las personas. La observancia o inobservancia de los mismos permiten establecer si un tratamiento de datos se está o no realizando de manera leal, lícita, transparente y adecuada.

La LGPDPPSO incorporó los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales, los cuales hacen parte de los principios creados por diversas entidades internacionales.

Los principios sobre el tratamiento de datos personales son herramientas muy valiosas para garantizar, en la práctica, la efectiva protección de los derechos de los titulares de los datos personales frente al tratamiento de su información. Adicionalmente, dichos principios se constituyen en un límite al tratamiento indebido de los datos personales y en un instrumento hermenéutico para la correcta interpretación y aplicación de la LGPDPPSO.

El reto siguiente será garantizar que los principios se apliquen en la práctica porque son el eje para que la protección de los derechos de las personas sea una realidad. Aunque es importante, no es suficiente la expedición de normas porque ellas no tienen efectos mágicos. Por eso, se deben concentrar esfuerzos para que los objetivos de la nueva ley no sean formales, sino reales y concretos, de manera que las personas realmente se beneficien de la misma.

Por eso, el principio de responsabilidad cobra cardinal importancia para lograr ese propósito pues exige que los sujetos obligados implementen medidas apropiadas, efectivas y verificables que les permitan probar el correcto cumplimiento de las normas sobre tratamiento de datos personales. Dichas medidas deben ser objeto de revisión y evaluación permanente para

medir su nivel de eficacia en cuanto al cumplimiento y el grado de protección de los datos personales. Para el efecto, el Programa Integral de Gestión de Datos (PIGD) se constituye en un mecanismo operativo para realizar todo lo necesario con miras a garantizar el debido tratamiento de los datos personales.

La ley y el principio de responsabilidad fracasarán si no se cumplen en la práctica. Por eso, insisto, debemos pasar de la retórica a la acción firme, seria y comprometida con el debido tratamiento de los datos personales.

El desafío de los sujetos obligados frente al principio de responsabilidad va mucho más allá de la mera expedición de documentos o políticas porque exige que se demuestre el cumplimiento real y efectivo de lo que dicen los mismos para que ellos no sean meros "saludos a la bandera" o simple "letra muerta". Con este principio se quiere que tantas promesas sobre tratamiento de datos sean una realidad comprobable y no un engaño o meros discursos sin aplicación práctica y concreta.

Finalmente, dejo planteada la siguiente reflexión: la información se ha convertido en un activo tan valioso y relevante que, en mi opinión, estamos migrando hacia una sociedad en la que se da más importancia a los datos que a las personas y la protección de sus derechos humanos. Hacia allá nos están llevando quienes viven de la industria del dato, pero ¿es hacia allá adónde queremos llegar?, ¿todo lo tecnológicamente posible es socialmente deseable?, ¿vale la pena acostumbrarnos a la expropiación de nuestros datos y de nuestros derechos humanos en nombre de la innovación y de la economía digital? Debemos estar alertas porque estamos a un paso de alcanzar la "cosificación del ser humano" en donde las personas no serán tratadas como tales sino como objetos o mercancía. Tanto *lobby* o cabildeo sobre la materia ponen de presente que el derecho de la protección de datos es el derecho de los derechos o, por lo menos, el derecho del siglo XXI. Por eso no debemos minimizar su importancia ni dejar que se banalice.

## Referencias

Asamblea General de las Naciones Unidas. (1990). *Principios rectores para la reglamentación de los ficheros computadorizados de datos personales. Resolución 45/95 de 14 de diciembre*.

Asia-Pacific Economic Cooperation. (2004). *Marco de privacidad del Foro de Cooperación Económica Asia Pacífico (APEC)*. Disponible en: https://www.sellosdeconfianza.org.mx/docs/marco_de_privacidad_APEC.pdf

Cavoukian, A. (2011). *Privacy by design: los 7 principios fundamentales*. [Archivo PDF]. Disponible en: https://www.acc.com/chapters/euro/upload/7foundationalprinciples-spanish.pdf, [fecha de consulta: 1 de mayo 2018].

Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. (2009). *Estándares internacionales para la protección de la privacidad en relación con el tratamiento de datos de carácter personal. (Resolución de Madrid)*.

García, A. (2007). La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado. *Boletín Mexicano de Derecho Comparado*, Universidad Nacional Autónoma de México, nueva serie, año XL, núm. 120, septiembre-diciembre, pp. 743-778.

Red Iberoamericana de Protección de Datos. (2017). *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*.

Red Iberoamericana de Protección de Datos. (2006). *Autorregulación y protección de datos personales*.

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), publicado en el *Diario Oficial de la Unión Europea,* L 119, el 4 de mayo de 2016.

Remolina, N. (2013). *Tratamiento de datos personales: aproximación internacional y comentarios a la ley 1581 de 2012*. Bogotá: Legis Editores.

Remolina, N. (2015). “El principio de accountability en el Gobierno Obama y en el contexto Iberoamericano”. Disponible en: https://habeasdatacolombia.uniandes.edu.co/?p=1804

Remolina, N. (2015). “Accountability y el compromiso gerencial en el tratamiento de datos personales”. Disponible en: https://habeasdatacolombia.uniandes.edu.co/?p=1886

Organización para la Cooperación y el Desarrollo Económicos. (2013). *Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales*.

Organización de los Estados Americanos. (2015). *Principios de la OEA sobre la privacidad y la protección de datos personales con anotaciones*. Adoptado en el 86º Período Ordinario de Sesiones del 23-27 de marzo. Río de Janeiro, Brasil, OEA/Ser.Q CJI/doc. 474/15 rev.2.

# CAPÍTULO II
# DE LOS DEBERES

***Artículo 31.*** *Con independencia del tipo de sistema en el que se encuentren los datos personales o el tipo de tratamiento que se efectúe, el responsable deberá establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad.*

***Artículo 32.*** *Las medidas de seguridad adoptadas por el responsable deberán considerar:*

*I. El riesgo inherente a los datos personales tratados;*

*II. La sensibilidad de los datos personales tratados;*

*III. El desarrollo tecnológico;*

*IV. Las posibles consecuencias de una vulneración para los titulares;*

*V. Las transferencias de datos personales que se realicen;*

*VI. El número de titulares;*

*VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento, y*

*VIII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.*

***Artículo 33.*** *Para establecer y mantener las medidas de seguridad para la protección de los datos personales, el responsable deberá realizar, al menos, las siguientes actividades interrelacionadas:*

*I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión;*

*II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales;*

*III. Elaborar un inventario de datos personales y de los sistemas de tratamiento;*

*IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros;*

*V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable;*

*VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales;*

*VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, y*

*VIII. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.*

***Artículo 34.*** *Las acciones relacionadas con las medidas de seguridad para el tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión.*

*Se entenderá por sistema de gestión al conjunto de elementos y actividades interrelacionadas para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el tratamiento y seguridad de los datos personales, de conformidad con lo previsto en la presente Ley y las demás disposiciones que le resulten aplicables en la materia.*

***Artículo 35.*** *De manera particular, el responsable deberá elaborar un documento de seguridad que contenga, al menos, lo siguiente:*

*I. El inventario de datos personales y de los sistemas de tratamiento;*

*II. Las funciones y obligaciones de las personas que traten datos personales;*

*III. El análisis de riesgos;*

*IV. El análisis de brecha;*

*V. El plan de trabajo;*

*VI. Los mecanismos de monitoreo y revisión de las medidas de seguridad, y*

*VII. El programa general de capacitación.*

***Artículo 36.*** *El responsable deberá actualizar el documento de seguridad cuando ocurran los siguientes eventos:*

*I. Se produzcan modificaciones sustanciales al tratamiento de datos personales que deriven en un cambio en el nivel de riesgo;*

*II. Como resultado de un proceso de mejora continua, derivado del monitoreo y revisión del sistema de gestión;*

*III. Como resultado de un proceso de mejora para mitigar el impacto de una vulneración a la seguridad ocurrida, y*

*IV. Implementación de acciones correctivas y preventivas ante una vulneración de seguridad.*

***Artículo 37.*** *En caso de que ocurra una vulneración a la seguridad, el responsable deberá analizar las causas por las cuales se presentó e implementar en su plan de trabajo las acciones preventivas y correctivas para adecuar las medidas de seguridad y el tratamiento de los datos personales si fuese el caso a efecto de evitar que la vulneración se repita.*

***Artículo 38.*** *Además de las que señalen las leyes respectivas y la normatividad aplicable, se considerarán como vulneraciones de seguridad, en cualquier fase del tratamiento de datos, al menos, las siguientes:*

*I. La pérdida o destrucción no autorizada;*

*II. El robo, extravío o copia no autorizada;*

*III. El uso, acceso o tratamiento no autorizado, o*

*IV. El daño, la alteración o modificación no autorizada.*

***Artículo 39.*** *El responsable deberá llevar una bitácora de las vulneraciones a la seguridad en la que se describa ésta, la fecha en la que ocurrió, el motivo de ésta y las acciones correctivas implementadas de forma inmediata y definitiva.*

***Artículo 40.*** *El responsable deberá informar sin dilación alguna al titular, y según corresponda, al Instituto y a los Organismos garantes de las Entidades Federativas, las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales, en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados puedan tomar las medidas correspondientes para la defensa de sus derechos.*

***Artículo 41.*** *El responsable deberá informar al titular al menos lo siguiente:*

*I. La naturaleza del incidente;*

*II. Los datos personales comprometidos;*

*III. Las recomendaciones al titular acerca de las medidas que éste pueda adoptar para proteger sus intereses;*

*IV. Las acciones correctivas realizadas de forma inmediata, y*

*V. Los medios donde puede obtener más información al respecto.*

***Artículo 42.*** *El responsable deberá establecer controles o mecanismos que tengan por objeto que todas aquellas personas que intervengan en cualquier fase del tratamiento de los datos personales, guarden confidencialidad respecto de éstos, obligación que subsistirá aún después de finalizar sus relaciones con el mismo.*

*Lo anterior, sin menoscabo de lo establecido en las disposiciones de acceso a la información pública.*

## COMENTARIO

**Andrés Velázquez**[36]

### I. Antecedentes

Vivimos en una sociedad donde cada día se tratan millones de datos personales. Sin el uso de nuestra información personal casi ninguno de los servicios de los que disponemos podría funcionar. Para cualquier actividad

[36] Con apoyo de Juan Carlos Carrillo, director de PWC México.

nos piden datos relacionados con nuestra esfera privada y la información personal que cedemos hace posible desarrollar actividades cotidianas.

El acceso a las tecnologías de la información se ha generalizado, por lo que el uso y tratamiento de la información personal no es un asunto menor, al contrario, es un tema en el que la seguridad, identificada como ciberseguridad, es un tema prioritario que debe estar omnipresente cuando se trata de recolección, resguardo, uso, manejo y transferencia de datos. Las preguntas que deben hacerse las personas que intervienen en cualquiera de las fases mencionadas son: ¿qué importancia tiene la ciberseguridad en la fase que está bajo mi responsabilidad?, ¿y qué impacto tiene una vulneración?

Para responder esas preguntas se necesita construir un nuevo paradigma para la protección de datos personales que contemple el tipo de sistema en el que se encuentran éstos o el tipo de tratamiento que se efectúe, como lo plantea el artículo 31 de este capítulo.

Para ello se requiere de una nueva lógica en el tratamiento de los datos personales que tome en cuenta la educación, concientización, socialización y elaboración de todo un andamiaje adecuado que permita salvaguardar y proteger los derechos personales, porque ante una sociedad dinámica y cada vez más digital existen una serie de implicaciones no sólo de hecho, sino también de derecho que pueden poner en riesgo el ejercicio y disfrute de otros derechos humanos.

## II. Relevancia temática y contexto

Hoy somos personas digitales y nuestra personalidad digital tiene dos dimensiones: aquella a través de la cual establecemos una relación directa mediante el pleno ejercicio de derechos, trámites y servicios con las instituciones del Estado, y la que tiene que ver con nuestra capacidad de ser consumidores de la información.

La ley, en cuanto a los deberes, es condición necesaria pero no suficiente, falta su implementación para lo que se requiere tener conocimiento de una arquitectura, es decir, de la estructura que sustenta a la protección de los datos personales desde los ámbitos jurídico, tecnológico y humano, que atienda a una visión sistémica de la protección de los datos.

La implementación de la ley implica retos y para ello se requiere conocimiento. Las disposiciones contenidas en este capítulo las agrupo en cuatro puntos que se convierten en premisas básicas para el cumplimiento de la ley: qué, cómo, quién y cuándo.

El *qué* tiene que ver con los datos personales y éstos con la tríada de la seguridad, compuesta por la confidencialidad, integridad y disponibilidad, cuidando que no se den sus opuestos, esto es, que los datos sean públicos, que sean editables y que no haya acceso a ellos.

El *cómo*, desde el punto en el que nos encontramos, implica la transición de un ambiente físico (que contiene una base de datos, un archivo o un sistema) a uno lógico que consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas. El objetivo es restringir el acceso a los programas y archivos, asegurar que los usuarios no puedan modificar los programas ni los archivos que no les correspondan, así como garantizar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto, analizando periódicamente los mismos.

Existen diferentes técnicas para lograr los objetivos en la seguridad lógica: identificación y autenticación (identificación es cuando el usuario se da a conocer en el sistema y autenticación es la verificación que se realiza en el sistema sobre esta identificación); el establecimiento de roles en el manejo de la información (algunos ejemplos serían el programador, el líder del proyecto, el administrador del sistema, etc.); las limitaciones a los servicios (por ejemplo, las licencias para el uso de un software); la modalidad de acceso (especificaciones para el uso de escritura, lectura, modificar, borrar, etc.); así como la ubicación y los horarios (especificar en dónde y en qué período de tiempo).

El *cómo* por sus características conduce al quién y esto implica un responsable general que tiene que concientizar, implantar controles y segregar el acceso y, a partir de él, a otras personas con sus respectivas competencias que tienen que ver con el análisis de riesgos (desde la perspectiva cuantitativa y cualitativa), políticas, guías, estándares, así como métodos y procesos para garantizar la ciberseguridad, entendida como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger a los activos de la organización y a los usuarios en el *ciber entorno*.

El *cuándo* tiene que ver con el momento o la circunstancia en la que se encuentra ese *quién* dentro del ambiente físico o lógico donde está presente el riesgo inherente, la sensibilidad de los datos, el desarrollo tecnológico, las posibles consecuencias de una vulneración para los titulares, las transferencias de datos personales que se realicen, el número de titulares, las vulneraciones previas ocurridas en los sistemas de tratamiento y el riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.

## III. Análisis del contenido

**1. Tipo de sistemas, deber de adoptar medidas de seguridad y evitar afectaciones.** El artículo 31 de la LGPDPPSO lo podemos dividir en tres partes: el tipo de sistema y su estado; la seguridad para la protección de datos (considerando al capital humano y a la tecnología) y evitar una afectación hacia los datos personales.

Del primer punto, el tipo de sistema y su estado, debemos considerar que los sistemas en cada sujeto obligado son diferentes en su funcionalidad, bases técnicas y tamaño de la base de datos personales. Esto significa que habrá un reto importante para homologar la protección de los datos, ya que no necesariamente se cuenta con los mismos presupuestos, tecnología, recursos humanos y capacitación para su manejo.

Para el segundo punto sobre la seguridad para la protección de datos, la ley se aboca a los ámbitos administrativo, físico y técnico. El más complejo será el administrativo, ya que tenemos que adentrarnos en el capital humano que está a cargo del cumplimiento de la ley, pues es quien administra los recursos y toma las decisiones de cualquier índole. Por ello, el responsable tiene un rol fundamental y para desarrollarlo debe contar con una capacitación constante para entender la evolución de las medidas de seguridad administrativas, físicas y técnicas e involucrar a toda la institución. Es claro que las medidas físicas son las más fáciles de entender y poner en práctica. Esto requerirá de un inventario de datos personales, pero también de un registro de quién o quiénes los administrarán, así como de las medidas de control para asegurarlos. Respecto a las medidas técnicas, la tecnología está en permanente evolución y hay cambios en hardware y software que permiten proteger los datos como lo marca la ley. Para atender esta disposición se deberá crear una estrategia que plantee cómo hacer uso de la tecnología y que considere medidas de seguridad, no sólo del repositorio de datos personales o base de datos, sino también de los mecanismos de transmisión de la información a los administradores y hasta los terceros involucrados.

Cada institución ha tratado de implementar la seguridad de una forma diferente, por ello es necesario difundir la definición y características de los diferentes tipos de seguridad. En algunas organizaciones ven a todos los tipos de seguridad como una sola área; en otras, los separan y sufren cambios con el paso del tiempo, por lo que cada vez es más importante tener una perspectiva integral y generar una estrategia que involucre a todos los tipos de seguridad, partiendo de lo siguiente: (1) Los datos personales siempre se encuentran en un lugar físico (aun en el caso de los datos digitales) dentro de un servidor informático o varios; por lo mismo, la seguridad física debe ser uno de los puntos por considerar desde la visión de riesgos. Las medidas

de seguridad física siempre tendrán que ser superiores para los datos personales sensibles y mayores a las utilizadas para otro tipo de información no personal. (2) La seguridad física vista fuera del contorno de la seguridad para la protección de los datos personales puede afectar a la privacidad, por lo tanto, siempre se debe mantener un equilibrio entre la seguridad y la privacidad. La privacidad debe utilizar a la seguridad, sin embargo, un exceso de seguridad puede afectar a la privacidad. (3) La seguridad administrativa engloba procesos técnicos y físicos que contribuyen a minimizar los riesgos. Este ámbito está estrechamente relacionado con el entendimiento de la ley y del contexto, por lo que la capacitación del capital humano se convierte en un factor prioritario para dar cumplimiento al artículo 31 de esta ley, porque sin conocimiento no hay estrategia.

El tercer punto habla de integridad, confiabilidad y disponibilidad, aspectos básicos de la seguridad informática, que no son solamente técnicos, sino también organizacionales, legales, económicos y sociales, por lo que no es adecuado y correcto aglutinar en un único valor a los tres componentes de la seguridad para establecer el cálculo del riesgo, ya que cada aspecto tiene un tratamiento diferente desde la perspectiva de las soluciones que hay que utilizar para proteger dichas características.

El artículo 31 nos plantea dos retos: uno de índole técnica y otro conceptual. Para el primero se debe conocer el tipo de tecnología con la que se cuenta y sus alcances; para el segundo, un conocimiento en forma de capacitación que permita en la práctica el cumplimiento de la disposición. La capacitación debe ir en dos sentidos: general y particular. Es decir, todos los empleados deben recibir una capacitación sobre aspectos generales de la ley al menos una vez por año y los nuevos colaboradores en sus primeros 90 días. En el sentido particular, todo colaborador que tenga dentro de sus funciones el contacto con datos personales deberá recibir una capacitación específica de cómo dentro de sus organizaciones se protegerán los datos personales, esto es, deberá existir capacitación dependiendo de la sensibilidad, volumen y tecnología para cada empleado.

**2. Criterios que deberán ser considerados en la adopción de medidas de seguridad.** El artículo 32 de la LGPDPPSO establece que las medidas de seguridad adoptadas por el responsable deberán considerar lo siguiente:

*I. El riesgo inherente a los datos personales tratados.*

La Metodología de Análisis de Riesgo BAA del IFAI[37] (ahora INAI), señala que el responsable de los datos personales debe identificar los tipos de datos que

[37] Instituto Federal de Acceso a la Información y Protección de Datos. (2014). *Metodología de Análisis de Riesgo BAA*. [Archivo PDF]. Disponible en: https://sontusdatos.org/wp-content/uploads/2013/04/ifai-metodologia-de-Riesgo-BAA_2014.pdf

se tratan, la sensibilidad de los mismos y el número de titulares para determinar el valor de riesgo inherente de los datos para un tercero no autorizado. Sin embargo, muchas veces no se considera que el riesgo inherente sea una constante, por lo que medirlo deberá ser un proceso permanente.

Para efectos cuantitativos, según la metodología, el nivel de riesgo inherente tiene que ver con la cantidad de personas en un sistema de tratamiento de datos personales, las cantidades van desde 500 hasta 500 mil.

A partir de esos criterios se debe considerar la relación del tipo de datos con el nivel de riesgo correspondiente, considerando el tipo de riesgo, el nivel inherente y el volumen de titulares. No es lo mismo un dato personal de riesgo bajo con un dato no sensible y un volumen elevado, a un dato sensible con un nivel de riesgo alto y un volumen reducido. Si bien, en ambos casos podría generarse una afectación, la magnitud de la misma establece su criticidad, por lo que se deben establecer las medidas apropiadas para identificar, mitigar y reducir el posible impacto que tendrán los riesgos en los activos de información a partir del riesgo inherente.

*II. La sensibilidad de los datos personales tratados.*

En la práctica, un dato no sensible puede convertirse en sensible por el tratamiento que se le otorgue, por lo tanto debería hablarse de tratamiento sensible de los datos, más que de datos sensibles. Esto implica tener presentes las siguientes preguntas: qué, dónde y quién tiene acceso a los datos; así como la finalidad (para qué) y el tratamiento (qué se hace con ellos) para lo que dichos datos fueron solicitados originalmente y para lo cual el titular dio el consentimiento. De la misma manera, será necesario ubicar el contexto ya que un dato aislado quizá no sea sensible, por lo que el riesgo no debe medirse sólo por el tipo de dato sino por la interacción entre ellos.

*III. El desarrollo tecnológico.*

La inversión en tecnología para la protección de datos personales debe ser constante, un grave error que las instituciones han cometido en el pasado es el realizar una sola inversión al inicio de su programa y después dejarlo como producto terminado. La protección de datos es un proceso sin fin y no un proyecto con tiempos específicos.

El desarrollo tecnológico debe verse desde dos perspectivas: la inversión y sus consideraciones (deberá ir al menos relacionado con dos factores: el volumen de los datos personales y la sensibilidad de los mismos), así como la inversión y su alcance.

Para atender este aspecto se desarrolló en los noventa la Privacidad por Diseño,[38] una trilogía de aplicaciones que engloban: sistemas de tecnologías de la información, prácticas de negocios responsables y diseño físico e infraestructura en red. La desarrolladora, Ann Cavoukian, directora ejecutiva del Instituto de Privacidad y Big Data (Ryerson University, Canadá) argumentó que la privacidad por diseño promueve la visión de que el futuro de la privacidad no puede ser garantizado sólo por cumplir con los marcos regulatorios y planteó siete principios fundamentales:[39] ser proactivo, no reactivo; que la privacidad sea parte integral del sistema, sin disminuir su funcionalidad; evitar la dualidad privacidad vs seguridad, demostrando que sí es posible tener ambas al mismo tiempo; seguridad *extremo a extremo* que implica la protección de ciclo de vida completo; visibilidad y transparencia para asegurar a todos los involucrados que cualquiera que sea la práctica de negocios o tecnología involucrada está operando de acuerdo a las promesas y objetivos declarados, y está sujeta a verificación independiente; respeto por la privacidad de los usuarios, esto es mantener un enfoque centrado en el usuario.

La privacidad desde el diseño propone que las cuestiones de protección de datos y privacidad se tomen en consideración desde la fase inicial, en el momento mismo del diseño de un producto o servicio; con ello se consigue, no sólo una mayor eficacia en la protección de los derechos de los afectados, sino también evitar algo que sucede con demasiada frecuencia: la reconversión de la norma a la tecnología, lo que lleva consigo altos costos para su rediseño y adaptación. El reto será entonces, ¿cómo sistematizamos el análisis de este riesgo?

### *IV. Las posibles consecuencias de una vulneración para los titulares.*

Una prioridad es mejorar la comunicación, así como la visibilidad y comprensión de las políticas, acciones que, en última instancia, permitirán responder más rápidamente a eventos indeseados e inesperados, así como ayudar al personal de la organización a asegurar sus activos, definir la postura hacia la protección de la información frente a accesos no autorizados, modificación, divulgación, destrucción o robo. Estos cuatro escenarios no sólo deben verse desde la perspectiva tecnológica, sino también humana, porque finalmente las personas son las que manejan la tecnología y los sistemas. Por ejemplo, muchas organizaciones contratan *outsourcing* para el desarrollo de sus aplicaciones internas, ¿y si éstas llegaran a manos de alguien más? La tecnología no necesariamente falló, la vulneración se da en el ámbito físico.

---

[38] GEV Asesores Internacionales, S.C. (2014). *Privacy by design para fomentar la figura del encargado*, septiembre 15, núm. 141. [Archivo PDF]. Disponible en: https://prosoft.economia.gob.mx/Imagenes/ImagenesMaster/Estudios%20Prosoft/FREF_23.pdf, [fecha de consulta: 8 de mayo 2018].

[39] Cavoukian, A. (2009). *Privacy by Design, The 7 Foundational Principles*. [Archivo PDF]. Disponible en: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf, [fecha de consulta: 8 de mayo 2018].

Para atender posibles consecuencias de una vulneración se deben considerar diversos escenarios que partan de lo ya conocido, pero también, y más importante, que contemplen lo que sucede en otros lugares (geografía) y sus características (análisis de lo sucedido, alcances, variaciones, etc.). Se necesitará un tercero que pueda apoyar en tener una visión externa del problema, una visión refrescada de la situación para que entienda los efectos de la vulneración.

*V. Las transferencias de datos personales que se realicen.*

El detalle con el que se pueda llevar a cabo este paso depende, en gran medida, del momento en que se realice la transferencia y para qué. Si una organización no conoce y comprende completamente los flujos de los datos personales que utiliza y cómo se usan, este hecho sería, en sí mismo, un grave riesgo para la privacidad que debería eliminarse mediante las tareas de documentación apropiadas.

La claridad con la que se expongan todos estos apartados es fundamental y para ello, además de utilizar un lenguaje claro, directo y comprensible, es de máxima importancia la inclusión de material gráfico que explique, de forma visual y resumida, los flujos de información. Algunos apartados básicos que deberían abordarse y documentarse son: la importancia de la información para la organización; identificación de los aspectos especialmente relevantes para la privacidad de las personas y que sean susceptibles de generar más riesgos o dificultar el cumplimiento normativo; una descripción detallada de los medios de tratamiento y de las tecnologías que se utilizarán y, en particular, de aquellas que introduzcan mayores riesgos para la privacidad; las categorías de datos personales que se van a tratar, finalidades para las que se usarán, necesidad de su uso y colectivos afectados, quién accederá a cada categoría de datos personales y los motivos y justificaciones para ello; así como los flujos de información: recolección, circulación dentro de la organización y fuera de la misma, y recepciones de datos personales procedentes de otras organizaciones.

Si fuera necesario, se debe incluir información y diagramas adicionales para ilustrar aspectos como el control de acceso o la conservación o destrucción de los datos personales. Los datos procedentes de estudios o auditorías anteriores o de inventarios de activos pueden resultar relevantes y muy útiles para ayudar en la confección de documentación adecuada.

*VI. El número de titulares.*

Como se mencionó en la fracción I del artículo 32, el nivel de riesgo inherente de cada tipo de dato se determina de acuerdo con la sección, identificación y clasificación de los datos personales mientras que el volumen de titulares se calcula acotando la cantidad de personas en un sistema de tratamiento de

datos personales. Al definir el nivel de riesgo inherente por cada tipo de dato y el volumen de titulares se podrá identificar el nivel de riesgo, el cual servirá para determinar los controles que debe considerar el responsable para la protección de datos personales. De acuerdo con la Metodología de Análisis de Riesgo BAA (IFAI, 2014), se han establecido cinco niveles posibles con valor numérico del 1 al 5 donde 1 es el nivel más bajo y 5 el más alto. Por ejemplo, el riesgo por tipo de dato nivel 3 ocurre cuando el nivel de riesgo inherente de los datos personales sea medio y se tenga de 50 mil personas en adelante; el nivel de riesgo inherente de los datos personales sea alto y se tenga de cinco mil personas en adelante.

*VII. Las vulneraciones previas ocurridas en los sistemas de tratamiento.*

Cuando se hace una respuesta a incidentes hay que entender que es necesario regresar a la operación cuanto antes, pero manteniendo evidencia de lo encontrado y permitiendo que las áreas de auditoría y contraloría realicen la documentación para presentarla a la autoridad cuando requiera la información del incidente. Considerar las vulneraciones previas y contar con la documentación de éstas facilita el conocimiento para generar políticas proactivas en lugar de reactivas.

Muchas veces las organizaciones no aceptan que han sido vulneradas y no lo reportan internamente por lo que no hay un aprendizaje sobre el pasado.

*VIII. El riesgo por el valor potencial cuantitativo o cualitativo que pudieran tener los datos personales tratados para una tercera persona no autorizada para su posesión.*

Para estimar el valor potencial de los datos se deben considerar los tipos de datos personales, la sensibilidad de los mismos y el número de personas de quienes se tratan dichos datos. La interrelación de estos factores puede ayudar a calcular el riesgo por el valor potencial cuantitativo o cualitativo y, además, determina el beneficio y accesibilidad que considera una tercera persona no autorizada para la posesión de los datos, para la cual el anonimato es un factor prioritario que está determinado por el nivel de riesgo del tipo de entorno desde el que se tiene acceso a los datos; esto reitera la importancia de una estrategia de seguridad.

**3. Actividades para la protección de datos personales.** El artículo 33 de la LGPDPPSO establece las actividades que el responsable deberá realizar respecto a la protección de datos personales, las cuales consisten en lo siguiente:

*I. Crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión.*

La política de seguridad es fundamental y debe contener al menos componentes digitales y físicos. Sin una política de seguridad, no se podrá fortalecer la política de privacidad. Para establecerla se debe tener en cuenta quién será el responsable de crearla, en qué estándar o mejor práctica estará basada y cuáles son sus ámbitos de aplicación. Una política sin control, monitoreo y sanciones no sirve.

La evolución tecnológica es un elemento determinante: no es lo mismo la tecnología de 2005 y la cantidad de datos almacenados en ese año a las condiciones actuales. Por ejemplo, a fin de modernizar el Sistema de Ahorro para el Retiro (SAR), en marzo de 2015 la CONSAR introdujo el Expediente Electrónico Único que mejora la atención pues permite realizar trámites en la Cuenta AFORE. En el sector salud se tiene desde 2010 el Expediente Clínico Electrónico (ECE) que contiene información sobre medicación, historia del paciente, protocolos clínicos y recomendaciones de estudios específicos.

Es recomendable contar con una política rectora de carácter gerencial que determine el compromiso de la dirección con la seguridad de la información, establezca la importancia de los activos y permita conocer el qué y porqué una organización planea protegerlos. Esta política debe estar soportada por otro grupo de políticas de carácter técnico, de las cuales pueden derivar guías o procedimientos que describen cómo se deben hacer las cosas y pueden considerar sistemas operativos, aplicaciones, red, administración, planes de negocio, dispositivos tecnológicos y seguridad física (elementos que están en evolución por lo que las políticas deben adecuarse al contexto y sus circunstancias).

Dentro de la misma política tiene que existir un punto en el que se establezca su revisión periódica, considerando factores internos y externos que determinen la actualidad u obsolescencia.

### *II. Definir las funciones y obligaciones del personal involucrado en el tratamiento de datos personales.*

El tratamiento de los datos personales requiere la participación activa de los altos directivos, la interrelación puede ser horizontal, vertical o mixta, dependiendo de las responsabilidades y prácticas ejercidas.[40] La intención es garantizar que el uso y los riesgos sean gestionados adecuadamente y verificar que los recursos de la empresa sean utilizados de manera responsable.

Las funciones y obligaciones del personal involucrado dependerán mucho de la organización, su tamaño, estructura y cultura particular. Sin embargo, se debe contar con representantes con capacidad de decisión (uno general y otro de seguridad) y comisionados cualificados de las áreas de TIC, negocios o de los departamentos a los que más afecte el tratamiento de los datos personales dentro de la organización.

[40] Quesada, J. y Velázquez, A. (2017). *Normatividad Bancaria 2017*. México: Editorial Porrúa.

*III. Elaborar un inventario de datos personales y de los sistemas de tratamiento.*

Un inventario de las bases de datos tendrá en cuenta los diversos tipos de datos almacenados (la naturaleza de los datos del empleado, del usuario, datos que le pertenecen a los usuarios y datos cuya propiedad se comparte con otra organización) y dónde se almacenan éstos; por ejemplo: servidores, dispositivos móviles, computadores, en la nube, etc., así como su ubicación geográfica. Existen procesos para poner al día el inventario con el propósito de que refleje los cambios en las bases de datos. Si bien contar con un registro ayuda a tener un control de la información, es importante tener presente que éste implica contar con medidas de seguridad ya que es un compendio de qué, quién, cómo, cuándo e incluso para qué, por lo que tanto las autoridades como los sujetos obligados deben estar conscientes de ello y tomar medidas en consecuencia.

*IV. Realizar un análisis de riesgo de los datos personales, considerando las amenazas y vulnerabilidades existentes para los datos personales y los recursos involucrados en su tratamiento, como pueden ser, de manera enunciativa más no limitativa, hardware, software, personal del responsable, entre otros.*

Si una organización no conoce o no comprende completamente los flujos de los datos personales que utiliza, este hecho sería, en sí mismo, un grave riesgo para la privacidad que debería eliminarse mediante las tareas de documentación apropiadas.

El análisis de riesgo puede incluir la identificación de aquellos aspectos especialmente relevantes para la privacidad de las personas y que sean susceptibles de generar más riesgos o de dificultar el cumplimiento normativo. También, debe contemplar los medios de tratamiento y las tecnologías que se utilizarán, en particular aquellas que introduzcan mayores riesgos para la privacidad como las categorías de datos personales que se van a tratar, su finalidad, necesidad de su uso y los colectivos que afecta.

Igualmente se debe considerar quién accederá a cada categoría de datos personales y los motivos y justificaciones para ello, así como los flujos de información: recolección, circulación dentro de la organización, sesiones fuera de la misma y recepciones de datos personales procedentes de otras organizaciones.

*V. Realizar un análisis de brecha, comparando las medidas de seguridad existentes contra las faltantes en la organización del responsable.*

El detalle con el que se pueda llevar a cabo depende en gran medida del momento en que se realice. Si el análisis tiene lugar en la fase inicial del proyecto (estudio de viabilidad, establecimiento de objetivos y requerimientos

generales, definición genérica de funcionalidades, etc.) la información con la que se cuente será todavía limitada y, por ello, es posible que también lo sea el resultado de este paso. Si éste fuera el caso, habría que volver a repasar y actualizar esta fase en cuanto lo permita el avance y desarrollo del proyecto y se disponga de información adicional más detallada para estimar cómo impacta la nueva información en las decisiones alcanzadas inicialmente.

Los datos procedentes de estudios o auditorías anteriores o de inventarios de activos pueden resultar relevantes y muy útiles en la confección de documentación adecuada que pondrán de manifiesto los objetivos, actores, categorías de datos que se tratan, tecnologías utilizadas, comunicaciones a terceros, necesidad de utilizar o no todos los datos previstos, necesidad que tienen los participantes de acceder y utilizar datos personales o categorías de datos personales específicas, etc.

*VI. Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, así como las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales.*

Un plan de trabajo implica tener identificados los riesgos para la protección de datos personales y en función de ello realizar una cuantificación de los mismos en dos aspectos: 1) probabilidad de que sucedan y 2) nivel de impacto en la privacidad que tendría su materialización.

El plan de trabajo debe tener un enfoque preventivo que considere las circunstancias y entorno del tratamiento de datos personales. Entre las medidas para el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales se deben considerar y atender las deficiencias en los niveles de seguridad, el uso de identificadores que revelan información del afectado, las deficiencias en la protección de la confidencialidad de la información, la falta de formación del personal sobre las medidas de seguridad que están obligados a adoptar y sobre las consecuencias que se pueden derivar de no hacerlo.

*VII. Monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales.*

La seguridad debe ser una parte integral de toda la estructura de la organización, no sólo para cubrir las necesidades actuales (o conocidas), sino también las futuras, a partir de una serie de acciones básicas: la alineación estratégica, así como la administración de los riesgos y los recursos. Para ello se requiere el apoyo de la alta dirección, la asignación de los recursos adecuados y de la definición de una estrategia que guíe las iniciativas de seguridad que deben

estar alineadas con los requerimientos y procesos de la organización, los resultados de la evaluación de riesgos y requisitos regulatorios.

Una vez establecido el proceso, se debe monitorear y revisar de manera periódica para mitigar los riesgos y reducir el posible impacto que tendría en los activos de información. Para la mayoría de las organizaciones, el establecimiento de un gobierno de seguridad de la información eficaz es una tarea primordial para integrar los esfuerzos aislados de seguridad que puedan existir, para hacer frente a la vulnerabilidad y amenazas a las que están sujetos los datos personales.

*VIII. Diseñar y aplicar diferentes niveles de capacitación del personal bajo su mando, dependiendo de sus roles y responsabilidades respecto del tratamiento de los datos personales.*

En la medición del desempeño se debe monitorear y reportar métricas de seguridad de la información para garantizar que se alcancen los objetivos. También se deben realizar evaluaciones de riesgos periódicos como parte de un programa global de administración de riesgos y establecer una estructura de seguridad para asignar individualmente roles y responsabilidades.

**4. Sistema de gestión.** Por su parte, el artículo 34 de esta ley general establece que las acciones relacionadas con las medidas de seguridad respecto al tratamiento de los datos personales deberán estar documentadas y contenidas en un sistema de gestión, que es un conjunto de reglas y principios relacionados entre sí de forma ordenada para contribuir a la gestión de procesos generales o específicos de una organización, por lo tanto, debe estar documentado y considerar situaciones como el desarrollo tecnológico, la cantidad de datos generados y cómo puede afectar a los interesados cuando se cedan o comuniquen a terceros, ya sea entregándolos, recibiéndolos o poniéndolos en común por cualquier medio.

Con un sistema de gestión se puede simplificar la interacción y la comunicación entre las distintas áreas para el manejo de los datos personales y asegurarse que todos en la organización trabajan para cumplir los objetivos. La documentación forma parte de la estrategia de seguridad y ciberseguridad porque la documentación adquiere un carácter proactivo que contribuye a mitigar los riesgos, ya que si se conoce la evolución tecnológica y la interacción entre las áreas de una organización, se puede tener el control de los datos generados y su posible vulneración.

**5. Documento de seguridad.** El artículo 35 de la LGPDPPSO establece los elementos mínimos que deberá contener el documento de seguridad elaborado por el responsable.

Tomando en cuenta la importancia que tiene que la entidad defina las necesidades de sus grupos de interés y la valoración de los controles precisos para mantener la seguridad de la información, se debe establecer una política que tenga en cuenta el marco general del funcionamiento de la entidad, sus objetivos institucionales y que se adapte a las condiciones específicas y particulares para que sea aprobada y guiada por la dirección.

Una buena política es concisa, legible, sencilla de comprender, corta, flexible, de fácil cumplimiento para todos los involucrados sin excepción y debe enmarcar los principios que guían las actividades dentro de la entidad.

**6. Actualización del documento de seguridad.** Por otra parte, el artículo 36 de la LGPDPPSO establece los supuestos en los que el responsable deberá actualizar el documento de seguridad.

La actualización debe establecer procedimientos para generar, asignar, distribuir, modificar, almacenar y dar de baja a usuarios y claves de acceso para la operación del sistema de datos personales; actualización de información contenida en el sistema de datos personales; procedimientos de creación de copias de respaldo y de recuperación de datos; bitácoras de acciones llevadas a cabo en el sistema de datos personales; procedimiento de notificación, gestión y respuesta ante incidentes y procedimiento para la cancelación de un sistema de datos personales.

**7. Vulneraciones a la seguridad.** El artículo 37 de la LGPDPPSO indica las labores que deberá realizar el responsable en caso de una vulneración a la seguridad.

Debe producirse un cambio en la mentalidad de quienes representan a las instituciones y organizaciones para que documenten las vulneraciones. La documentación facilita el análisis de riesgo y el análisis de brecha, y éstos a su vez permiten hacer un mapeo que conduzca a saber por qué ocurrió, en qué fase o área se originó, si es el caso; pero, sobre todo, revisar para establecer nuevas medidas de seguridad. Si no se conocen las deficiencias no se pueden aplicar acciones correctivas que, vistas desde una perspectiva sistémica, pueden plantearse como preventivas después del incidente.

Por su parte, el artículo 38 de esta ley señala, además de las que se encuentren en las leyes respectivas y normatividad aplicable, los supuestos de vulneración de seguridad, entre las que se mencionan: la pérdida o destrucción; el robo, extravío o copia; el uso, acceso o tratamiento y el daño, alteración o modificación que se realice de manera no autorizada.

Ante cualquier escenario que pueda vulnerar la información personal bajo el resguardo de instituciones públicas y organizaciones privadas se debe considerar, al menos, cinco aspectos: (1) que la tecnología y el capital humano están interrelacionados y, en determinados casos, pueden funcionar como un binomio, considerando que un alto porcentaje de las vulneraciones no se debe a la falta de herramientas tecnológicas adecuadas sino a las malas prácticas por parte de los trabajadores; (2) que la incorporación de nuevas tecnologías o políticas públicas requieren que, desde su diseño, se implementen las medidas necesarias para que los datos personales sean protegidos y tratados de manera adecuada; (3) que siempre se mantengan actualizados los equipos de cómputo y sistemas de información; (4) que se cuente con copia de los datos personales y de la información crítica, así como con la validación y la realización de pruebas periódicamente para comprobar que los respaldos funcionen, y (5) la atención a las noticias sobre ciberseguridad y protección de datos personales para estar informado sobre nuevas amenazas y poder implementar las medidas de seguridad más asertivas.

De igual manera, el artículo 39 de la LGPDPPSO establece que el responsable deberá llevar una bitácora de las vulneraciones a la seguridad que debe contener los datos completos del responsable, encargado o usuario; el modo de autenticación; fecha y hora en que se realizó o intentó el acceso; el sistema de datos personales accedido; las operaciones o acciones llevadas a cabo dentro del sistema de datos personales; así como la fecha y hora en que se realizó la salida del sistema.

El objetivo de la bitácora es documentar procedimientos y criterios enfocados a garantizar el nivel de seguridad exigido, así como generar, asignar, distribuir, modificar, almacenar y dar de baja usuarios y claves de acceso para la operación del sistema de datos personales.

El encargado deberá llevar un registro de incidentes en el que se consignen los procedimientos realizados para la recuperación de los datos o para permitir una disponibilidad del proceso, indicando la persona que resolvió el incidente, la metodología aplicada y los datos recuperados.

La bitácora puede ser física o electrónica. Es importante tener en cuenta la información que se incluye y considerar medidas de seguridad para la salvaguarda de ésta teniendo en cuenta una pregunta fundamental: ¿Qué pasaría si la bitácora es objeto de los supuestos del artículo 38 de esta ley?

Por otra parte, el artículo 40 establece la obligación del responsable de informar al titular y, en su caso, al INAI y a los organismos garantes de las

entidades federativas, sobre las vulneraciones que afecten significativamente los derechos patrimoniales o morales.

En California, donde se creó la primera regulación donde se exigen las normas anteriores, al principio las empresas se negaron a notificar, porque pensaban que eso significaría informar que su seguridad estaba mal o que los clientes se cambiarían de compañía. Pero es importante que informen para salvaguardar la seguridad de sus clientes o usuarios, ya que la vulneración de base de datos personales afecta más a los titulares de la información que a las instituciones que la resguardan.

El artículo 41 de la ley establece, por su parte, lo mínimo que el responsable deberá informarle al titular para cumplir con la ley, demostrar el compromiso con la seguridad y transparencia en el manejo de los datos y para que los titulares puedan minimizar el posible impacto de las vulneraciones para tomar las medidas necesarias y evitar daños, reales o potenciales (como cambiar contraseñas, números de cuenta, cancelar tarjetas de crédito o débito, entre otros). Omitir la notificación de vulneraciones es negarle a los afectados la oportunidad de adoptar medidas oportunas para protegerse de peligros reales y latentes.

**8. Deber de confidencialidad.** Finalmente, el artículo 42 de la LGPDPPSO señala la obligación del responsable de establecer controles para que todas las personas que intervengan en cualquier fase del tratamiento de datos personales guarden confidencialidad, aún después de finalizar la relación entre el responsable y el titular de los datos personales.

El deber de secrecía, respecto de los datos personales tratados, es una obligación que corresponde al responsable del fichero, físico o informático, al encargado del tratamiento (si lo hubiera) y a todos aquellos que intervienen en cualquier fase del manejo de datos de carácter personal. No debe confundirse este deber con el secreto profesional al que están sometidas determinadas personas en función de la profesión que ejercen, pues el deber de secrecía aplica para cualquier persona que intervenga en el tratamiento de los datos.

Se recomienda la inclusión de cláusulas específicas en esta materia en los contratos laborales donde los trabajadores se comprometen a guardar secreto sobre la información confidencial y los datos de carácter personal de los que tenga conocimiento en el ejercicio de las funciones que le sean encomendadas, de conformidad con lo establecido en la ley. El trabajador está obligado a atender las instrucciones relativas a la seguridad de los datos de carácter personal contenidas en las políticas de seguridad por el responsable de seguridad.

## IV. Conclusiones

De todo lo anterior debemos destacar dos puntos importantes: uno tiene que ver con la materia y la parte sustantiva de la ley, y el otro, con los retos que va a implicar la interpretación de la ley. En relación al segundo, los sujetos obligados van a requerir una capacitación focalizada porque se establecen obligaciones particulares, lo que supone un conocimiento y aterrizaje de la materia mucho más específico, a fin de que se encuentren en posibilidad de cumplir con sus obligaciones, atendiendo a la dinámica propia de los tiempos actuales: las redes sociales, el mundo conectado, la información que viaja y se difunde a millones de personas con un solo clic, lo que requiere que para la protección de los datos personales sea necesario crear políticas internas para la gestión y tratamiento de los datos personales hasta monitorear y revisar de manera periódica las medidas de seguridad implementadas, así como las amenazas y vulneraciones a las que están sujetos los datos personales, pasando por el análisis de riesgo, el análisis de brecha y la capacitación del personal bajo su mando.

Debemos tomar en cuenta que el peligro para la privacidad del individuo no radica en que se acumule información sobre él, sino en que pierda la capacidad de disposición sobre quién y con qué objeto se transmite. Además, debemos considerar que la informática ha constituido una revolución en el ámbito de los métodos tradicionales para la organización, registro y uso de la información. La dimensión cuantitativa de la información que puede ser almacenada y transmitida es de tal magnitud que ha dado lugar a un auténtico cambio cualitativo que obliga a considerar la protección de los datos personales como un derecho de última generación.

Actualmente, el modelo de gestión Gobierno, Riesgo y Cumplimiento (GRC) promueve la unificación de criterios, la coordinación de esfuerzos y la colaboración entre todos los involucrados en la dirección de una organización a través de lograr la integración de los órganos responsables de la gestión de riesgos, control interno y cumplimiento, asignación puntual de roles y clara responsabilidad de funciones, formalización de canales de comunicación adecuada, aplicación de un enfoque basado en riesgos y la implementación de un programa de cumplimiento que, desde mi punto de vista, implica: inversión, evolución tecnológica, capital humano y seguridad desde un enfoque jurídico. Lo anterior, porque la LGPDPPSO es considerada un avance jurídico debido a que la población proporciona cotidianamente datos de su ámbito privado a las instituciones públicas, ya sea para el ejercicio de derechos, recibir un bien o servicio público o para el cumplimiento de sus deberes.

La inversión es parte de lo anterior porque se debe destinar un capital para lograr el equilibrio entre invertir en la protección de datos personales, asumir los niveles de riesgo y monitorear el posible abuso de datos personales. Por ello, para fortalecer la responsabilidad proactiva de quienes tratan datos personales en los sectores público y privado resultan especialmente útiles enfoques como el de la Privacidad desde el Diseño, que propugna que las cuestiones de protección de datos y privacidad se tomen en consideración desde la fase inicial, es decir, desde el diseño de un producto o servicio. Con ello se consigue no sólo una mayor eficacia en la protección de los derechos de los afectados, sino también la reconvención de la tecnología, lo que implica altos costos para su rediseño y adaptación.

La evolución tecnológica tiene que ver con la inversión *per se* y con la comunicación móvil, las redes sociales y el cómputo en la nube, entre otras tecnologías (que agrupan el *big data*, el Internet de las cosas, etc.), que han dado lugar a nuevos riesgos para el manejo de datos personales tanto para las organizaciones como para sus colaboradores que tienen un doble papel: manejar y resguardar los datos personales y cuidar que su derecho a la tríada de la seguridad sea respetado. Por lo anterior, las organizaciones deben implantar proactivamente estrategias de protección de datos (de acuerdo con su perfil de riesgo) y capacitar a sus colaboradores en el manejo de los datos personales, así como para administrar mejor los riesgos y obligaciones de cumplimiento, también se requiere conocer los derechos relativos al tratamiento de los datos personales (como los derechos ARCO) —aspecto relacionado con la premisa *cuándo* de esta ley.

En este marco, la ciberseguridad se presenta como un círculo concéntrico destinado a proteger los datos personales.

## Referencias

Agencia Española de Protección de Datos. (2014). *Guía para una Evaluación de Impacto en la Protección de Datos Personales*. [Archivo PDF] Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf, [fecha de consulta: 2 de mayo 2018].

Cavoukian, A. (2009). *Privacy by Design, The 7 Foundational Principles*. [Archivo PDF]. Disponible en: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf, [fecha de consulta: 2 de mayo 2018].

Chalico, C. (marzo, 2011). Asuntos relevantes sobre protección de datos personales para 2011, *Boletín Fiscal Ernst & Young*.

García, A. (septiembre-diciembre, 2007). La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado. *Boletín Mexicano de Derecho Comparado*, Universidad Nacional Autónoma de México, nueva serie, año XL, núm. 120, pp. 743-778.

GEV Asesores Internacionales, S.C. (2014). *Privacy by design para fomentar la figura del encargado*. [Archivo PDF]. Disponible en: https://prosoft.economia.gob.mx/Imagenes/ImagenesMaster/Estudios%20Prosoft/FREF_23.pdf, [fecha de consulta: 2 de mayo 2018].

Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal. (2011). *Retos de la protección de datos personales en el sector público*. [Archivo PDF]. Disponible en: http://procesos.finanzas.cdmx.gob.mx/oip/Consulta/pdf/Cuadro7.pdf

Instituto Federal de Acceso a la Información y Protección de Datos. (2014). *Metodología de Análisis de Riesgo BAA*. [Archivo PDF]. Disponible en: https://sontusdatos.org/wp-content/uploads/2013/04/ifai-metodologia-de-Riesgo-BAA_2014.pdf

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. *Protección de Datos Personales en el Sector Público.* [Presentación Power Point]. Disponible en: www.infoem.org.mx/doc/presentaciones/Taller_datos_personales.pptx

Magallanes, V. (julio-diciembre 2016). Derecho a la protección de datos personales. Su diseño constitucional, *Estudios en Derecho a la Información*, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, núm. 2, pp. 25-45. Disponible en: https://revistas.juridicas.unam.mx/index.php/derecho-informacion/article/view/10486/12651, [fecha de consulta: 2 de mayo 2018].

Martínez, E. (2011). *El derecho a la protección de datos personales en la Administración Pública Federal.* [Archivo PDF]. Disponible en: https://www.itei.org.mx/v3/micrositios/diplomado02/gdl/adjuntos/Sector_Publico_ITEI_18-19-nov-2011.pdf, [fecha de consulta: 2 de mayo 2018].

Qués, M. (2013). *Datos Personales y nuevas tecnologías. Serie estrategias en el aula para el modelo 1 a 1*. Argentina: Ministerio de Educación.

Quesada, J. y Velázquez, A. (2017). *Normatividad Bancaria* 2017. México: Editorial Porrúa.

Rouse, M. (2013). *Prevención de pérdida de datos (DLP)*. Disponible en: http://searchdatacenter.techtarget.com/es/definicion/Prevencion-de-perdida-de-datos-DLP, [fecha de consulta: 2 de mayo 2018].

SonTusDatos.Org. (2017). *Encuesta sobre políticas de notificación de vulneraciones de datos personales en el sector privado*. [Archivo PDF]. Disponible en: https://sontusdatos.org/wp-content/uploads/2017/01/170118-reporte_encuesta-vf-1.pdf, [fecha de consulta: 2 de mayo 2018].

# TÍTULO TERCERO
# DERECHOS DE LOS TITULARES Y SU EJERCICIO

# CAPÍTULO I
# DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN

***Artículo 43.*** *En todo momento el titular o su representante podrán solicitar al responsable, el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales que le conciernen, de conformidad con lo establecido en el presente Título. El ejercicio de cualquiera de los derechos ARCO no es requisito previo, ni impide el ejercicio de otro.*

***Artículo 44.*** *El titular tendrá derecho de acceder a sus datos personales que obren en posesión del responsable, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento.*

***Artículo 45.*** *El titular tendrá derecho a solicitar al responsable la rectificación o corrección de sus datos personales, cuando estos resulten ser inexactos, incompletos o no se encuentren actualizados.*

***Artículo 46.*** *El titular tendrá derecho a solicitar la cancelación de sus datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no estén en su posesión y dejen de ser tratados por este último.*

***Artículo 47.*** *El titular podrá oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo, cuando:*

*I. Aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular, y*

*II. Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a*

*evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.*

## COMENTARIO

**Paulina del Pilar Gutiérrez**

Los artículos 43 al 47 de la LGPDPPSO comprenden el grupo de derechos por medio de los cuales se garantiza el control de las personas sobre sus datos personales. Los derechos ARCO son la materialización del derecho a la autodeterminación informativa, aquel bajo el cual las personas deciden y tienen control sobre la difusión, manejo, uso y aprovechamiento de su información personal[41] por parte de los sujetos obligados descritos en el artículo primero de la ley general.[42]

Cabe destacar que, aun cuando los derechos ARCO son la manifestación de dicho control y personifican el carácter nuclear de la especial protección otorgada a los datos personales, es ineludible reconocer que su acelerado desarrollo normativo e interpretativo en el sistema europeo ha generado impactos perjudiciales en el ejercicio de la libertad de expresión e información en Latinoamérica y México , esto se debe a una preferencia hacia la protección de la intimidad, el honor y la reputación sin profundizar en los límites y excepciones que como regla contrastan con el régimen de protección de datos personales.

### I. Antecedentes

El desarrollo de los estándares de protección que anteceden el reconocimiento de los derechos ARCO en México son principalmente de carácter histórico-normativo. Por ello, con el objetivo de conocer cuál es el origen tutelar de estos derechos, así como su extensión cuando conviven con los límites de otros derechos humanos, abordaremos en este apartado los antecedentes en el marco normativo mexicano y los elementos tutelares que delimitaron en un principio sus alcances.

[41] Piñar, J. y Ornelas, L. (2013). "Introducción, La protección de datos como derecho fundamental", en Ornelas Núñez, L. y Piñar, J. (Coords.) *La Protección de Datos Personales en México*. México: Tirant Lo Blanch México, pp. 20-71.

[42] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, "Artículo 1. […] 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. […]".

La protección de datos personales adquirió relevancia en los sesenta y ochenta una vez que el incremento en el uso de las computadoras permitió procesar información de las personas y el comercio transfronterizo produjo un procesamiento electrónico de datos susceptibles de uso o abuso por terceros. Dichos fenómenos tecnológicos impactaron directamente en la privacidad de los individuos[43] y dieron pie al primer reconocimiento constitucional del derecho a la autodeterminación informativa mediante un fallo emitido por tribunal alemán en 1983.

La relevancia del precedente constitucional alemán radica en la argumentación que da origen a este concepto como derecho fundamental y que se centra en el vínculo que existe entre la intimidad y el desarrollo de la personalidad en conexión con la autodeterminación informativa de las personas en la medida en que cada una decide sobre la información que comparte sobre su esfera personal y privada.[44]

Es así como podemos referir al esquema con el cual se definió la autodeterminación informativa, el derecho a decidir la forma y los límites protectores bajo los cuales: 1) decidimos qué información personal se conozca; 2) a quién se le entrega, y 3) cómo o bajo qué circunstancias proporcionamos nuestra información personal[45] a entidades públicas o privadas.

A partir de entonces, y durante un período que abarca de 1980 a 2007, diversas recomendaciones, directrices, directivas y resoluciones,[46] emitidas por diferentes actores internacionales y autoridades[47] han instituido un conjunto de principios, deberes y derechos —en específico los llamados derechos ARCO— con la intención de proteger la información con el objetivo de que su tratamiento no lesione los derechos y libertades de los titulares, de manera particular lo relacionado con su intimidad, honor, honra, debido proceso, entre otros.[48]

---

[43] Rudgard, S. (2012). *Origins and historical context of data protection law*. [Archivo PDF]. Disponible en: https://iapp.org/media/pdf/publications/European_Privacy_Chapter_One.pdf, [fecha de consulta: 2 de mayo 2018].

[44] Korff, D. *et al.* (2010). *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments. Country Studies: Germany*. Comisión Europea. Disponible en: https://publications.europa.eu/en/publication-detail/-/publication/9c7a02b9-ecba-405e-8d93-a1a8989f128b/language-en.

[45] Bazán, V. (1999). El habeas data, el derecho a la autodeterminación informativa y la superación del concepto preinformático de la intimidad. *Boletín Mexicano de Derecho Comparado*, Universidad Nacional Autónoma de México, nueva serie, año XXXII, núm. 94, enero-abril, pp. 13-76. Disponible en: https://revistas.juridicas.unam.mx/index.php/derecho-comparado/article/view/3575.

[46] En reiteradas ocasiones la Agencia Española de Protección de Datos ha manifestado que la protección de datos personales fue reconocida como un derecho autónomo e independiente en la sentencia 292/2000 del Tribunal Constitucional Español.

[47] La Organización para la Cooperación y el Desarrollo Económicos en 1980, el Parlamento Europeo y el Consejo de Europa en 1981 y 1995, la Organización de las Naciones Unidas en 1981, el Foro de Cooperación Económica Asia-Pacífico en 1999, Autoridades de Protección de Datos Personales en 2000 y 2009; la Red Iberoamericana de Protección de Datos Personales en 2007.

[48] Remolina, N. (2013). “Los derechos de Acceso, Rectificación, Cancelación y Oposición en la Ley de datos personales y su Reglamento”, en Ornelas Núñez, L. y Piñar, J. (Coords.), *La Protección de Datos Personales en México*. Tirant Lo Blanch, México, pp. 132-152.

Es mediante la estandarización de los niveles de protección de los datos personales que se constituyen los derechos ARCO como prerrogativas fundamentales para salvaguardar las libertades democráticas de las personas. Sin embargo, es fundamental precisar que los derechos de acceso y rectificación fueron las primeras facultades otorgadas y se conocen como derechos de primera generación de los datos personales,[49] con contenido específico y estandarizado desde 1980. Por el contrario, los derechos de cancelación y oposición han sido susceptibles a un desarrollo de estandarización asimétrico, en la medida en que su procedencia y operatividad coinciden o se encuentran con los límites de otros derechos fundamentales como la libertad de expresión e información.

Antes de profundizar en los comentarios relacionados con los ámbitos de aplicación de los derechos ARCO y sus puntos de inflexión con la protección y ejercicio de otros derechos humanos, hagamos un breve recuento de los antecedentes de estos derechos en México.

Una vez que los derechos ARCO se convierten en las previsiones sustantivas de la autodeterminación informativa y la protección de los datos centrada en la intimidad de las personas, México adopta por primera vez los aspectos generales de la protección de datos personales en la LFTAIPG publicada en julio de 2002.[50]

Es a través de las reformas constitucionales a los artículos 6º y 16 que los derechos ARCO adquieren un carácter formal y material en México. En un primer momento los derechos de acceso y rectificación reconocidos mediante su adición al artículo sexto constitucional en julio de 2007 y posteriormente los derechos ARCO en su conjunto con la reforma al artículo 16 en junio de 2009. Esta última derivó en la promulgación del primer marco legal de carácter especial en materia de protección de datos personales en posesión de particulares en México: la LFPDPPP, publicada el 5 de julio de 2010, la cual dio reconocimiento expreso a la autodeterminación informativa de las personas en su artículo primero.

Ambas reformas establecieron los siguientes elementos: 1) el vínculo formal entre la vida privada y la protección a los datos personales como un derecho fundamental complementario a la manifestación de ideas y la libertad informativa; 2) el derecho de toda persona a tener acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos;[51] y 3) ampliaron el derecho de toda persona a la protección de sus datos personales

[49] *Idem.*

[50] Peschard, J. (2013). “Introducción”, en Ornelas Núñez, L. y Piñar, J. (Coords.), *La Protección de Datos Personales en México*. Tirant Lo Blanch, México, pp. 14 -27.

[51] Fracciones II y III adicionadas al artículo 6º constitucional a través de su reforma publicada el 20 de julio de 2007.

en el marco de la prohibición a injerencias en su vida privada bajo la protección autónoma de los derechos ARCO.[52]

Finalmente, cinco años después de que México adoptara formalmente un marco constitucional de protección a los datos personales, se publicó la LGPDPPSO el 26 de enero de 2017. Esta ley es producto de la reforma de 2014 en materia de transparencia, acceso a la información pública y protección de datos personales en posesión de sujetos obligados.[53]

Ciertamente, el predictamen de la ley general fue objeto de diversas recomendaciones técnicas basadas en preocupaciones sustantivas y adjetivas que tenían por objeto evitar un perjudicial desequilibrio entre el derecho a la protección de datos personales —aunque reconocido como derecho autónomo basado en la intimidad— y el derecho a la libertad de expresión e información en México.[54] Cabe subrayar que dicha problemática permanece vigente en tanto las observaciones fueron excluidas durante el proceso de diseño y discusión de este cuerpo normativo a cargo de la Cámara de Diputados y el Senado de la República.

## II. Relevancia temática y contexto

La entrada en vigor de la ley general representa un avance normativo en función del desarrollo "asimétrico que existe en los estándares de protección de datos personales"[55] en el mundo.[56] No sólo por la tutela especial que adquieren los titulares sobre el control de su información personal sometida a tratamiento por las autoridades —y demás sujetos obligados— en ámbitos automatizados, computarizados y tecnológicos, sino también, en contraste, por el potencial desequilibrio entre el derecho a la vida privada y el derecho a la libertad de expresión, si este último se excluye de la interpretación sistemática de los derechos ARCO.

---

[52] Párrafo segundo adicionado al artículo 16 constitucional a través de su reforma publicada el1 de junio de 2009.

[53] Cfr. El DECRETO por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, *Diario Oficial de la Federación,* 7 de febrero de 2014. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5332003&fecha=07/02/2014, [fecha de consulta: 2 de mayo 2018].

[54] ARTICLE19, R3D, FUNDAR, SonTusDatos.Org, CIMTRA, MI. 2016. "El Estado mexicano debe aprobar una ley que garantice efectivamente la protección de datos personales y no funja como medio indirecto para la restricción de otros derechos". Disponible en: https://articulo19.org/el-estado-mexicano-debe-aprobar-una-ley-que-garantice-efectivamente-la-proteccion-de-datos-personales-y-no-funja-como-un-medio-indirecto-para-la-restriccion-de-otros-derechos/.

[55] Maqueo, M. (2017). *Módulo I. Orígenes, vida privada, privacidad y datos personales*, sesión del Diplomado en Privacidad, Regulación y Gobernanza de Datos del Centro de Investigación y Docencia Económicas, impartido el 22 de septiembre.

[56] Cfr. Banisar, D. (2018). *National Comprehensive Data Protection/Privacy Laws and Bills 2018*. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416, [fecha de consulta: 2 de mayo 2018].

El acelerado avance normativo e interpretativo al que hacemos referencia a lo largo del texto tiene como fuente la resolución del Tribunal de Justicia de la Unión Europea (TJUE) en el caso *Costeja* o también conocido como *Google Spain*, a través del cual se realizó una interpretación extensiva del derecho de cancelación o eliminación de datos personales, con el objetivo de ordenar a la empresa Google desvincular el nombre del titular de la lista de resultados de información en los motores de búsqueda publicados por terceros y páginas web en línea.[57]

La relevancia del precedente europeo radica, en primer lugar, en la inédita propagación del concepto implementado en la sentencia denominado derecho al olvido y a través del cual el Tribunal europeo otorgó, como regla, la prevalencia del derecho de eliminación de datos personales sobre el interés general del derecho a la información.[58] Un concepto considerado ofensivo y agraviante en contextos como el latinoamericano[59] y una sentencia que omitió el estudio de otros derechos que pudieran verse afectados como el de libertad de expresión.[60]

Tal interpretación extensiva del derecho de cancelación conforme a la Directiva 95/46/CE dio pie a que el nuevo RGPD de la UE[61] dedicara un apartado específico al *derecho al olvido*, intensificando una preferencia desproporcionada por la eliminación de datos en línea y "causando un serio desequilibrio entre los derechos a la [libertad de] expresión y a la intimidad".[62]

Un segundo aspecto de relevancia del precedente europeo tiene su origen en el hecho de que el sistema de protección de datos personales mexicano, regido por intereses comerciales con Europa y sus consecuentes necesidades de estandarizar los esquemas de tutela, "ha tomado como referente el

---

57 Tribunal de Justicia de la Unión Europea. (2014). *Sentencia del Tribunal de Justicia* (Gran Sala) de 13 de mayo de 2014. Google Inc. vs Agencia Española de Protección de Datos Personales y Mario Costeja González. Disponible en: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES, [fecha de consulta: 2 de mayo 2018].

58 *Ibíd.*, pp. 311-313.

59 Bertoni, E. (2014). The Right to be Forgotten: an insult to Latin American History. *Huffington Post.* Disponible en: https://www.huffingtonpost.com/eduardo-bertoni/the-right-to-be forgotten_b_5870664.html, [fecha de consulta: 2 de mayo 2018].

60 Keller, D. (2017). El derecho al olvido de Europa en América Latina, en Del Campo, Agustina (Comp.), *Hacia una Internet libre de censura II*. Argentina: Centro de Estudios sobre Libertad de Expresión, Universidad de Palermo. [Archivo PDF]. Disponible en: http://www.palermo.edu/cele/pdf/investigaciones/Hacia_una_internet_libre_de_censura_II.pdf, [fecha de consulta: 2 de mayo 2018].

61 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), publicado en el *Diario Oficial de la Unión Europea,* L 119, el 4 de mayo de 2016, con aplicación obligatoria en los estados miembros de la Unión Europea a partir del 25 de mayo de 2018.

62 Keller, D., *Op. Cit.*

desarrollo de la Unión Europea (UE)"[63] sin reconocer expresamente que el mal denominado —por evitar llamarlo inexistente— *derecho al olvido* nace de esquemas diferenciados de protección a la vida privada, honra, reputación y libertad de expresión e información en México y en el Sistema Interamericano de Derechos Humanos (SIDH).

Al contrario, las intenciones por implementar en México la interpretación europea del derecho de cancelación (que se empleó en el caso Costeja) se han considerado perjudiciales para censurar información de interés público en línea a través de resoluciones que ordenaron a Google remover enlaces vinculados a noticias sobre potenciales actos de corrupción[64] y, por otro lado, incorporar el concepto o una regulación vaga e imprecisa del inexistente derecho al olvido[65] durante los procesos legislativos de esta ley general y la Constitución Política de la Ciudad de México[66] por mencionar algunos ejemplos.

Los precedentes anteriores son de particular relevancia en la medida en que se contraponen al contexto jurídico y sociopolítico mexicano, el cual se caracteriza por tener un margen jurídico interamericano de amplia protección a la libertad de expresión e información conforme al artículo 13 de la Convención Americana sobre Derechos Humanos (CADH) así como por una crisis de graves violaciones a derechos humanos, impunidad generalizada y corrupción en todos los niveles de gobierno.[67]

Por lo tanto, el derecho a la verdad y la memoria, en conjunto con la libertad de expresión e información, son un punto medular en el estudio y análisis sobre el ejercicio de los derechos ARCO en México, en especial si nos referimos a mecanismos jurídicos orientados a olvidar. "La población quiere recordar y no olvidar. En este sentido, es importante reconocer el contexto particular de la región y cómo un mecanismo legal como el llamado *derecho al olvido* y su incentivo para la desindexación puede afectar el derecho a la verdad y la memoria".[68]

---

[63] Maqueo, M. (2017). *Módulo I. Orígenes, vida privada, privacidad y datos personales*, sesión del Diplomado en Privacidad, Regulación y Gobernanza de Datos del Centro de Investigación y Docencia Económicas, impartido el 22 de septiembre.

[64] Red en Defensa por los Derechos Digitales (R3D). (2016). *Tribunal anula resolución del INAI sobre el falso derecho al olvido*. Disponible en: https://r3d.mx/2016/08/24/amparo-inai-derecho-olvido/, [fecha de consulta: 2 de mayo 2018].

[65] Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos. (2017). *Estándares para una internet libre, abierta e incluyente.* [Archivo PDF]. Disponible en: http://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf, [fecha de consulta: 2 de mayo 2018].

[66] Red en Defensa de los Derechos Digitales. (2016). *El erróneamente llamado derecho al olvido no es un derecho, es una forma de censura*. Disponible en: https://r3d.mx/2016/07/12/el-erroneamente-llamado-derecho-al-olvido-no-es-un-derecho-es-una-forma-de-censura/, [fecha de consulta: 2 de mayo 2018].

[67] Comisión Interamericana de Derechos Humanos. (2015). *Situación de los derechos humanos en México*. [Archivo PDF]. Disponible en: http://www.oas.org/es/cidh/informes/pdfs/Mexico2016-es.pdf, [fecha de consulta: 2 de mayo 2018].

[68] Comisión Interamericana de Derechos Humanos. (2017). *Estándares para una internet libre, abierta e incluyente*. [Archivo PDF]. Disponible en: http://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf, [fecha de consulta: 2 de mayo 2018].

## III. Análisis del contenido

Con el fin de describir y analizar los alcances del contenido material y formal de los derechos ARCO, consagrados en los artículos comentados, es necesario recordar que el derecho a la protección de datos personales nace de un proceso evolutivo del derecho a "la privacidad [y la intimidad] con el objeto de abordar problemáticas relacionadas con la recolección, el uso y la divulgación de información personal en posesión de gobiernos y actores privados en diversos sistemas de información".[69]

Por lo tanto, puede decirse que los derechos ARCO surgen como un mecanismo *ad hoc* diseñado para brindar control a los titulares sobre su información, orientado a salvaguardar una dimensión privada de sus vidas, expuesta por un procesamiento de información a cargo de terceros y susceptible de ser usada y aprovechada de manera abusiva o ilícita.

Irremediablemente, el derecho a la protección de datos personales forma parte del ámbito de protección del derecho a la privacidad y la intimidad, aun cuando éste haya adquirido el carácter de derecho fundamental autónomo. Tanto es así, que el desarrollo normativo europeo referido a lo largo del texto, en específico en lo que respecta al concepto *derecho al olvido*, se sustenta reiteradamente en las afectaciones a la vida privada de la persona en relación con el tratamiento de datos personales mediante procedimientos automatizados.[70]

En función de lo anterior, un primer enfoque crítico al esquema de protección de los derechos ARCO está centrado en los intentos por instrumentar la argumentación del caso *Costeja* en procesos legislativos en México sin reconocer que el derecho a la privacidad, y por ende la protección de datos personales y los derechos ARCO, están sujetos a las limitaciones permisibles reconocidas por el derecho internacional de los derechos humanos, mejor conocido como el test tripartito de legalidad, necesidad y proporcionalidad.[71]

La ley general no incorporó el test de necesidad y proporcionalidad en las limitaciones a la protección de datos personales enunciadas en el artículo sexto, únicamente estableció las circunstancias materiales enunciadas como aquellas "[...] por razones de seguridad nacional, [...] disposiciones de orden público, seguridad y salud pública o para proteger los derechos de terceros".

---

69 ARTICLE19. (2016). *The "Right to be Forgotten": Remembering Freedom of Expression*. [Archivo PDF]. Disponible en: https://www.article19.org/data/files/The_right_to_be_forgotten_A5_EHH_HYPERLINKS.pdf, [fecha de consulta: 2 de mayo 2018].

70 Véase nota 57.

71 Consejo de Derechos Humanos de la Organización de las Naciones Unidas. (2009). *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*. [Archivo PDF]. Disponible en: http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf, [fecha de consulta: 2 de mayo 2018).

Esta omisión tendrá un impacto directo en la garantía y ejercicio de los derechos ARCO en la medida en que convivan con otros derechos.

Particularmente en situaciones donde los derechos de acceso, cancelación y oposición requieran ser analizados a la luz de las limitaciones relacionadas con la protección de derechos de terceros, en especial con el derecho a la libertad de expresión y acceso a la información. La adopción expresa del test tripartito y la libertad de expresión e información como una excepción en la ley, representaba una oportunidad inédita para evitar restricciones arbitrarias a los derechos ARCO por parte de los sujetos obligados y garantizar que "las leyes de privacidad no [...] inhib[an] ni restrinj[an] la investigación y difusión de información de interés público".[72]

Sin embargo, para alcanzar niveles de progresividad significativos es necesario retomar un enfoque bajo el cual la privacidad, la protección de datos personales y la libertad de expresión e información son reconocidos como derechos que se fortalecen mutuamente, al igual que permanecen limitados exclusivamente cuando el test de legalidad, necesidad y proporcionalidad así lo haya determinado.[73]

Los planteamientos anteriores nos servirán para abordar los alcances y las posiciones encontradas en la interpretación y procedencia de cada uno de los derechos ARCO reconocidos en la ley general, así como la viabilidad de implementar medidas alternativas y menos perjudiciales o gravosas tanto para los derechos ARCO como para la libertad de expresión e información.

**1. Derecho de acceso.** Los derechos de acceso y rectificación son históricamente las primeras facultades otorgadas a los titulares de los datos.[74] Ciertamente, en ausencia del derecho de acceso, la rectificación y cualquier otro derecho estarían generalmente inhabilitados. Dicho de otra manera, el derecho de acceso a los datos personales es la vía de entrada a través de la cual el titular tiene conocimiento de los datos personales almacenados en los archivos, registros o bases de datos controladas y/o procesadas por los sujetos obligados.

De ahí la importancia que ostenta el derecho de acceso a los datos personales, el cual implica una obligación positiva del Estado centrada en garantizar que "[t]oda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privados y, en el caso de que fuere necesario, actualizarla, rectificarla y/o enmendarla".[75]

---

[72] Comisión Interamericana de Derechos Humanos. (2000). *Antecedentes e Interpretación de la Declaración de Principios*. Disponible en: http://www.oas.org/ES/CIDH/EXPRESION/showarticle.asp?artID=132&lID=2, [fecha de consulta: 2 de mayo 2018).

[73] ARTICLE19. (2017). *The Global Principles on Protection of Freedom of Expression and Privacy*. Disponible en: http://article19.shorthand.com/, [fecha de consulta: 2 de mayo 2018].

[74] Véase nota 48.

[75] Cfr. El principio 3 de la "Declaración de Principios sobre Libertad de Expresión" de la Comisión Interamericana de Derechos Humanos.

Sin embargo, aun cuando la procedencia del derecho de acceso a los datos personales se ha planteado como regla en la ley general, las limitaciones al derecho de acceso por razones de seguridad nacional, orden público y seguridad pública representan un sustancial desafío para evitar restricciones desproporcionadas a este derecho y, en su caso, oponerse al tratamiento ante potenciales abusos o violaciones a la vida privada, el debido proceso y la presunción de inocencia de las personas.

En específico, la problemática se ha centrado en la ausencia de mecanismos y salvaguardas efectivas que garanticen al titular, por un lado, tener conocimiento de intervenciones arbitrarias y desproporcionadas por parte de las instancias de seguridad, procuración y administración de justicia; y por el otro, poder acceder a controles que contrarresten un potencial abuso o aprovechamiento de los datos personales que éstas almacenan, procesan, remiten y usan sin la obligación de recabar el consentimiento, notificar al titular de manera diferida[76] respecto de la obtención y tratamiento de sus datos,[77] así como de consagrarse como una excepción a la procedencia del derecho de acceso.

En tales circunstancias, el titular tiene una reducción significativa en el umbral de protección especial de su derecho a acceder a la información sobre sí mismo, un derecho sin el cual está imposibilitado para interponer acciones de cancelación u oposición que limiten un tratamiento ilícito. En contraste, el alcance del esquema de protección de este derecho es limitado y también obstaculiza al titular el derecho de oponerse a la destrucción o eliminación de sus datos personales de los registros, archivos y bases de datos del sujeto obligado a fin de tener conocimiento posterior sobre su tratamiento y, en su caso, someterlo a escrutinio.[78]

**2. Derecho de rectificación.** El derecho de rectificación tiene por objeto remediar la divulgación, uso y aprovechamiento de datos inexactos, incompletos o desactualizados en los registros, archivos y bases de datos de los sujetos obligados. Por lo tanto, este derecho está íntimamente ligado con la obligación del responsable

[76] Véase nota 64.

[77] La notificación diferida es una medida reconocida internacionalmente como un medio para inhibir los riesgos de abuso en los casos donde las autoridades obtienen y tratan información personal de los titulares con fines de seguridad, procuración y administración de justicia. Esta medida ha sido recomendada por diversas organizaciones y organismos internacionales de derechos humanos como salvaguarda a la vigilancia de los titulares a través del tratamiento de datos personales en ámbitos tecnológicos y de telecomunicaciones. Cfr. Necessary and Proportionate Coalition. (2014). *Necessary and Proportionate, International Principles on the Application of Human Rights to Communications Surveillance*. Disponible en: https://necessaryandproportionate.org/principles, [fecha de consulta: 2 de mayo 2018].

[78] Estos casos pueden suscitarse principalmente cuando las instancias de seguridad, procuración y administración de justicia ejercen sus facultades establecidas en los artículos 189 y 190 de la Ley Federal de Telecomunicaciones y Radiodifusión, así como en aplicación de sus consecuentes lineamientos de colaboración en materia de seguridad y justicia, emitidos por el Instituto Federal de Telecomunicaciones.

de “mantener exactos, completos, correctos y actualizados los datos personales en su posesión” (artículo 23 de la LGPDPPSO), mejor conocida como el principio de calidad de los datos personales.

La exactitud en los datos se vincula con la veracidad de la información personal tratada por los sujetos obligados, es relevante en tanto el tratamiento de datos inexactos implica un uso, manejo, divulgación y aprovechamiento de datos falsos.[79] Entonces, el derecho de rectificación garantiza que el tratamiento de los datos personales sea consistente con la finalidad previamente establecida y evitar daños en los derechos y libertades del titular, o en su caso de terceros, en situaciones donde el tratamiento responda a los datos incorrectos.

Los beneficios del derecho de rectificación han sido recientemente retomados por las corrientes que se oponen al ejercicio del derecho de cancelación utilizado como medida excesiva para remediar afectaciones al honor, reputación y vida privada. Este debate será profundizado a detalle en el siguiente apartado.

**3. Derecho de cancelación y oposición.** La incorporación de nuevas tecnologías para la obtención, procesamiento, tratamiento y divulgación de información personal se ha traducido en riesgos para la protección de datos personales. Los derechos de cancelación y oposición parecen haberse incorporado como medidas para restringir de manera absoluta e irremediable la existencia de aquellos datos cuyo tratamiento contravenga las disposiciones legales o genere afectaciones en los derechos y libertades del titular.

Su desarrollo normativo e interpretativo se ha extendido al grado de importar el concepto europeo del *derecho al olvido* para solicitar la remoción absoluta de contenidos de acceso público en internet en México.[80] Es pertinente señalar que la remoción expande significativamente el concepto europeo para exigir ilegítimamente a periódicos y periodistas la eliminación de información,[81] incluso, la Relatoría Especial para la Libertad de Expresión, RELE (2017), ha dado cuenta de que “funcionarios [y figuras públicas] han recurrido a este concepto para eliminar información de interés público, instaurando en muchos casos la práctica de reemplazar acciones de calumnias e injurias ante los tribunales por acciones de oposición ante la autoridad de protección de datos personales”.

---

[79] Piñar, J. y Ornelas Núñez, L. (2013). “Introducción. La protección de datos como derecho fundamental”, en Ornelas, L. y Piñar, J. (Coords.), *La Protección de Datos Personales en México*. Tirant Lo Blanch, México, pp. 20-71.

[80] Véase nota 64.

[81] Diversas organizaciones de la sociedad civil mexicana han documentado la existencia de despachos privados que utilizan el concepto *derecho al olvido* para hostigar, amenazar e intimidar a medios y periodistas con el objeto de que eliminen información sobre personas específicas de sus portales. Generalmente se trata de información de interés público.

En tales circunstancias, el erróneamente llamado derecho al olvido es considerado como un mecanismo de censura que desconoce el "[...] impacto evidente en el derecho a la libertad de expresión, tanto en su dimensión individual como social, y en el derecho de acceso a la información por parte del público. La información removida no circula, lo que afecta el derecho de las personas a expresarse y difundir sus opiniones e ideas y el derecho de la comunidad a recibir informaciones e ideas de toda índole".[82]

Si bien el caso *Costeja* y la adopción del concepto referido especifica las circunstancias de los actores y el contenido involucrado en solicitudes de "desindexación" como a) información del titular agraviado b) disponible y procesada por los motores de búsqueda, c) publicada por terceros, merece atención reconocer los supuestos bajo los cuales este concepto puede prestarse a que los derechos de cancelación y oposición sean ejercidos ante los sujetos obligados con la intención de eliminar información fundamentalmente necesaria para clasificar, sistematizar, preservar y poner a disposición archivos históricos sobre violaciones de derechos humanos y al derecho internacional humanitario.[83]

En su momento, las recomendaciones técnicas entregadas a las comisiones dictaminadoras de la ley general se centraron justamente en establecer de manera expresa el derecho a la libertad de expresión e información como una excepción a la protección de datos personales; integrar la prueba de interés público; y establecer controles judiciales para la eliminación, cancelación, supresión u oposición de datos personales sobre información de interés público y archivos con un potencial carácter histórico.[84]

Resulta entonces preocupante que la ley general carezca de salvaguardas que garanticen la protección del derecho a la información ante solicitudes de titulares que hayan ostentado una calidad pública en el pasado o actualmente, como funcionarios, candidatos o cualquier individuo que realice o haya ejecutado actos de autoridad y ejerzan recursos públicos supuestos en los cuales debe existir una fuerte presunción en contra de sus solicitudes de desindexación y/o cancelación de información.[85]

La ley únicamente dispone de requisitos diferenciados para las solicitudes del derecho de cancelación y oposición en tanto el titular debe manifestar

---

82 Véase nota 65.

83 Comisión Interamericana de Derechos Humanos. (2014). *Derecho a la verdad en América*. [Archivo PDF]. Disponible en: http://www.oas.org/es/cidh/informes/pdfs/Derecho-Verdad-es.pdf, [fecha de consulta: 2 de mayo 2018].

84 Red en Defensa de los Derechos Digitales. (2016). *Pre-Proyecto de Dictamen de Ley General de Datos Personales, lejos de garantizar los derechos humanos*. Disponible en: https://r3d.mx/2016/03/10/pre-proyecto-de-dictamen-de-ley-general-de-datos-personales-lejos-de-garantizar-los-derechos-humanos/, [fecha de consulta: 2 de mayo 2018].

85 Véase nota 65.

las razones que motivan la supresión de sus datos y manifestar las causas legítimas que le orillen a solicitar el cese del tratamiento, así como el daño o perjuicio que le causa la persistencia del tratamiento.

Por lo tanto, y en pleno reconocimiento de que la protección de datos personales es una restricción legítima al derecho a la libertad de expresión e información cuando la eliminación de los datos suspende de manera definitiva intervenciones arbitrarias o ilícitas a la intimidad y la vida privada de las personas por parte de la autoridad, creemos que existen casos donde los criterios de exactitud, adecuación, relevancia y necesidad para la cancelación, supresión y oposición al tratamiento de los datos personales requieren ser complementados con el esquema de las restricciones permisibles, tanto para proteger la privacidad, la honra o la reputación, como para la libertad de expresión e información.

Es decir, estar legalmente establecida en una ley en sentido formal y material; ser necesaria e idónea, y proporcional; las limitaciones deben ser, además, ordenadas por un juez o autoridad jurisdiccional competente, independiente e imparcial con todas las garantías del debido proceso.[86]

Lo anterior no se plantea con la intención de generalizar los casos cuyo estudio deba quedar sometido a procedimientos complejos que se contraponen a contar con mecanismos sencillos y expeditos para ejercer los derechos ARCO, al contrario, se pretende evitar la eliminación excesiva y desproporcionada de información que podría no ser relevante o necesaria al momento de la solicitud del titular, pero determinante para el acceso a la justicia, el derecho a la verdad y la memoria, así como para preservar la información histórica de la sociedad mexicana.[87]

Por otro lado, también merece atención recuperar los supuestos donde la cancelación se convierte en el medio más adecuado para remediar daños severos en la vida privada de las personas, sobre todo aquellas afectaciones intensificadas por la exposición y predeterminación de conductas generadas por el tratamiento automatizado de los datos personales. Estos casos se caracterizan porque la información es difundida de manera ilegal, está disponible en el dominio público, generalmente se obtiene y es difundida sin el consentimiento de la persona afectada. De manera similar, habrá información cuya eliminación garantizará que sujetos obligados como instancias de seguridad, procuración y administración de justicia se abstengan de tratar

[86] *Ibíd.*, p. 35.

[87] ARTICLE19 ha documentado casos en los que nombres de funcionarios y víctimas involucradas en crímenes del pasado son testados de las versiones públicas de documentos de carácter histórico. La ley no contempla salvaguardas para evitar que solicitudes de cancelación u oposición remuevan de manera permanente la información testada, medida que evidentemente obstaculiza el acceso a datos e información personal revestida de interés público.

ilícitamente los datos obtenidos sin el conocimiento del titular. Sin embargo, estos casos también carecen de medidas como la notificación diferida para garantizar el acceso y eventual cancelación de los datos de los titulares en posesión de los sujetos obligados mencionados.

En concreto, existirán casos en los cuales sea necesario realizar ejercicios de ponderación de derechos para determinar la procedencia y operatividad del derecho de cancelación y oposición. Existen corrientes en contra del concepto derecho al olvido que proponen recurrir a medidas menos restrictivas y gravosas para el derecho a la libertad de expresión como lo es el derecho de rectificación.

Este último proporciona una solución cuyo objeto es modificar y corregir datos que sean equívocos y erróneos, sin generar daños irremediables al derecho de acceso a la información. Es preferible recurrir y otorgarle preferencia al derecho de rectificación antes de apelar a medidas legales orientadas a olvidar y remover información en contextos donde se mantienen legítimos reclamos de mayor acceso a información sobre la actividad gubernamental del pasado y graves violaciones de los derechos humanos.[88]

Asimismo, es relevante integrar en la discusión la existencia y vigencia de esquemas civiles de protección relacionados con afectaciones al honor, reputación y buen nombre que no deberían ser reemplazados por el régimen de protección de datos personales para eliminar información. Los organismos autónomos y el Poder Judicial están en una posición preferencial para determinar si la eliminación de la información está justificada y se trata de una medida proporcional que no impacta de manera lesiva la libertad de expresión e información.[89]

En función de lo anterior, y además de reiterar que existirán casos legítimos para eliminar de manera absoluta datos personales del titular, se recomienda tener criterios adicionales al estudio de las solicitudes de cancelación y oposición sustentadas en argumentos extensivos e importados del concepto europeo *derecho al olvido*:

1. El grado en el que la información en cuestión ostenta una evidente naturaleza privada, por ejemplo: detalles de la vida íntima y sexual, salud del titular, detalles bancarios, información sensible, entre otros.

2. La información reviste interés público o contribuye a debates en la materia, ya sean pasados, presentes o futuros.

3. El titular tiene una expectativa razonable de privacidad: conducta previa del interesado, consentimiento otorgado, la información podría ya estar en el dominio público y ahí debe permanecer.

[88] Véase nota 65.
[89] Véase nota 69.

4. Características del sujeto objeto de la solicitud: notoriedad o vulnerabilidad de la persona, son figuras públicas o funcionarios públicos.

5. Las características de los registros donde se encuentra la información.

6. Estudio del contenido, utilidad y consecuencias reales del daño alegado, a tal grado que interfiera con su vida privada y menoscabe su integridad personal.

7. La manera en que la información fue recopilada.[90]

Consecuentemente, la cancelación de datos personales y la oposición al tratamiento que pudiera derivar en censura, remoción de contenidos en línea y una medida para obstaculizar el acceso al derecho a la información, ya sea mediante un uso ilegítimo o extensivo del concepto europeo *derecho al olvido digital*, debe ser estrictamente de carácter excepcional, ordenada por un juez u órgano independiente que haya realizado una ponderación de derechos, y siempre y cuando, la prueba de interés público haya sido agotada. "La decisión por parte de una autoridad de eliminar información o bloquear motores de búsqueda sólo se puede basar en el hecho de que la forma de obtener dicha información o el contenido de la misma sea maliciosa, falsa, o produzca un serio daño a un individuo".[91]

## IV. Conclusiones

Consciente de que los comentarios vertidos en este capítulo podrían parecer contrarios a ciertos objetivos de la ley orientados a establecer procedimientos sencillos y expeditos para el ejercicio de los derechos ARCO, me parece importante destacar que una parte nuclear relacionada con la adopción de un marco normativo que brinda especial protección a la privacidad de las personas y a la protección de sus datos personales, es aquella en la que reconocemos que en ausencia de estos derechos la libertad de expresión e información está minada.

No obstante, los comentarios tienen la intención de recordar la esencia tutelar del derecho a la protección de datos personales concebida desde la autodeterminación informativa y construida para obtener el control de aquella información propia y susceptible a un uso y aprovechamiento ilícito por parte del responsable. Esta construcción de los derechos ARCO ha planteado límites desde sus orígenes, entre los cuales se encuentran los derechos de terceros.

---

[90] Criterios tomados del Test de siete elementos o *seven part test* promovido internacionalmente como el mecanismo adecuado para evitar un desequilibrio entre la libertad de expresión e información, la privacidad y la protección de datos personales en la era digital. Al respecto, véase el policy brief `*The Right to be forgotten´: Remembering Freedom of Expression* y *The Global Principles on Protection of Freedom of Expression and Privacy*, anteriormente citados.

[91] Véase nota 60.

Hoy en día, ante el acelerado desarrollo tecnológico, comercial y digital en el cual circulan y se procesan nuestros datos de carácter personal, el régimen de protección de datos personales encuentra puntos de inflexión con un derecho en particular: el derecho a la libertad de expresión e información, cuya relevancia y protección se reconocen al mismo nivel que la privacidad como un derecho fundamental tanto en espacios físicos como digitales.

Entonces, la necesidad de promover procesos locales de innovación interpretativa en la materia se vuelven prioritarios en tanto existan nociones y sistemas de protección diferenciados atribuibles a ambos derechos. El concepto *derecho al olvido* es incompatible con el sistema interamericano de derechos humanos. Resulta entonces contraproducente importar conceptos legales que materializarían una medida regresiva para la protección de ambos derechos en circunstancias donde se toman como conceptos amplios, con restricciones genéricas y en ausencia de un test de intereses públicos en compañía de la legalidad, necesidad y proporcionalidad de la medida.

De ahí la utilidad de integrar de manera expresa el derecho a la libertad de expresión como una excepción a la protección de datos personales, ya que ante un uso excesivo, ampliado e ilegítimo del erróneamente denominado *derecho al olvido*, el carácter medular de los derechos ARCO para la protección de datos personales se enfrenta a serias problemáticas asociadas al derecho de cancelación y oposición, mismas que ante una visión miope, reducen los casos de cancelación necesaria y legítima por una generalización de su ejercicio como mecanismos de censura.

Finalmente, me gustaría también mencionar que el reconocimiento de los derechos ARCO en el marco de la ley general y las fuentes del sistema de protección constitucional del cual provienen tienen las capacidades de reconciliar el potencial desequilibrio entre los derechos a la privacidad y la libertad de expresión, principalmente a través de mecanismos alternativos a la eliminación de información. Las personas que observan, cumplen, aplican e interpretan la ley general requieren tener presente que ambos derechos tienen limitaciones, son complementarios y se fortalecen mutuamente.

Así, la solución al creciente, y algunas veces retórico conflicto, entre el derecho a la protección de datos personales y la libertad de expresión e información tiene la solución en el desarrollo de sus propios límites y el mutuo reconocimiento como derechos fundamentales íntimamente vinculados.

## Referencias

ARTICLE19. (2016). *The "Right to be Forgotten": Remembering Freedom of Expression*. [Archivo PDF]. Disponible en: https://www.article19.org/data/files/The_right_to_be_forgotten_A5_EHH_HYPERLINKS.pdf, [fecha de consulta: 2 de mayo 2018].

ARTICLE19. (2016). *El Estado mexicano debe aprobar una ley que garantice efectivamente la protección de datos personales y no funja como medio indirecto para la restricción de otros derechos*. Disponible en: https://articulo19.org/el-estado-mexicano-debe-aprobar-una-ley-que-garantice-efectivamente-la-proteccion-de-datos-personales-y-no-funja-como-un-medio-indirecto-para-la-restriccion-de-otros-derechos/, [fecha de consulta: 2 de mayo 2018].

ARTICLE19. (2017). *The Global Principles on Protection of Freedom of Expression and Privacy*. Disponible en: http://article19.shorthand.com/, [fecha de consulta: 2 de mayo 2018].

Banisar, D. (2018). *National Comprehensive Data Protection/Privacy Laws and Bills 2018*. Disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416, [fecha de consulta: 2 de mayo 2018].

Bazán, V. (1999). El habeas data, el derecho a la autodeterminación informativa y la superación del concepto preinformático de la intimidad. *Boletín Mexicano de Derecho Comparado*, Universidad Nacional Autónoma de México, nueva serie, año XXXII, núm. 94, enero-abril, pp. 13-76. Disponible en: http://dx.doi.org/10.22201/iij.24484873e.1999.94.3575.

Bertoni, E. (2014). *The Right to be Forgotten: an insult to Latin American History. Huffington Post*. Disponible en: https://www.huffingtonpost.com/eduardo-bertoni/the-right-to-be-forgotten_b_5870664.html, [fecha de consulta: 2 de mayo 2018].

Comisión Interamericana de Derechos Humanos. (2000). *Antecedentes e Interpretación de la Declaración de Principios*. Disponible en: http://www.oas.org/ES/CIDH/EXPRESION/showarticle.asp?artID=132&IID=2, [fecha de consulta: 2 de mayo 2018).

Comisión Interamericana de Derechos Humanos. (2014). *Derecho a la verdad en América*. [Archivo PDF]. Disponible en: http://www.oas.org/es/cidh/informes/pdfs/Derecho-Verdad-es.pdf, [fecha de consulta: 2 de mayo 2018].

Comisión Interamericana de Derechos Humanos. (2015). *Situación de los derechos humanos en México*. [Archivo PDF]. Washington, DC. OEA/Ser. L./V/II. Doc. 44/15, 31 de diciembre. Disponible en: http://www.oas.org/es/cidh/informes/pdfs/Mexico2016-es.pdf, [fecha de consulta: 2 de mayo 2018].

Consejo de Derechos Humanos de la Organización de las Naciones Unidas. (2009). *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*. [Archivo PDF]. A/HRC/13/37, 28 de diciembre. Disponible en: http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf, [fecha de consulta: 2 de mayo 2018).

Directiva 95/45/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, publicada en el *Diario Oficial de las Comunidades Europeas,* L 281, el 23 de noviembre de 1995.

DOF. (junio, 2009). DECRETO por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. *Diario Oficial de la Federación*. [Archivo PDF]. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_187_01jun09.pdf, [fecha de consulta: 2 de mayo 2018].

DOF. (julio, 2014). Ley Federal de Telecomunicaciones y Radiodifusión, *Diario Oficial de la Federación*.

Keller, D. (2017). El derecho al olvido de Europa en América Latina, en Del Campo, Agustina (Comp.), *Hacia una Internet libre de censura II*. Argentina: Centro de Estudios sobre Libertad de Expresión, Universidad de Palermo. [Archivo PDF]. Disponible en: http://www.palermo.edu/cele/pdf/investigaciones/Hacia_una_internet_libre_de_censura_II.pdf, [fecha de consulta: 2 de mayo 2018].

Korff, D. (2010). *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments. Country Studies: Germany. Comisión Europea*. Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_A4_germany.pdf.

Maqueo, M. (2017). *Módulo I. Orígenes, vida privada, privacidad y datos personales*, sesión del Diplomado en Privacidad, Regulación y Gobernanza de Datos del Centro de Investigación y Docencia Económicas, impartido el 22 de septiembre.

Necessary and Proportionate Coalition. (2014). *Necessary and Proportionate, International Principles on the Application of Human Rights to Communications Surveillance*. Disponible en: https://necessaryandproportionate.org/principles, [fecha de consulta: 2 de mayo 2018].

Peschard, J. (2013). "Introducción", en Ornelas, L. y Piñar, J. (Coords.), *La Protección de Datos Personales en México*. México: Tirant Lo Blanch, pp. 14 -27.

Piñar, J. y Ornelas, L. (2013). "Introducción. La protección de datos como derecho fundamental", en Ornelas, L. y Piñar, J. (Coords). *La Protección de Datos Personales en México*. Tirant Lo Blanch, México, pp. 20 a 71.

Red en Defensa por los Derechos Digitales (R3D). (2016). *Tribunal anula resolución del INAI sobre el falso derecho al olvido*. Disponible en: https://r3d.mx/2016/08/24/amparo-inai-derecho-olvido/, [fecha de consulta: 2 de mayo 2018].

Red en Defensa de los Derechos Digitales. (2016). *El erróneamente llamado derecho al olvido no es un derecho, es una forma de censura*. Disponible en: https://r3d.mx/2016/07/12/el-erroneamente-llamado-derecho-al-olvido-no-es-un-derecho-es-una-forma-de-censura/, [fecha de consulta: 2 de mayo 2018].

Red en Defensa de los Derechos Digitales. (2016). *Pre-Proyecto de Dictamen de Ley General de Datos Personales, lejos de garantizar los derechos humanos*. Disponible en: https://r3d.mx/2016/03/10/pre-proyecto-de-dictamen-de-ley-general-de-datos-personales-lejos-de-garantizar-los-derechos-humanos/, [fecha de consulta: 2 de mayo 2018].

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), *Diario Oficial de la Unión Europea,* L 119, el 4 de mayo de 2016.

Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos. (2017). *Estándares para una internet libre, abierta e incluyente*. [Archivo PDF]. Disponible en: http://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf, [fecha de consulta: 2 de mayo 2018].

Remolina, N. (2013). "Los derechos de Acceso, Rectificación, Cancelación y Oposición en la Ley de datos personales y su Reglamento", en Ornelas, L. y Piñar, J. (Coords.), *La Protección de Datos Personales en México*. Tirant Lo Blanch, México, pp. 132 a 152.

Rudgard, S. (2012). *Origins and historical context of data protection law*. [Archivo PDF]. Disponible en: https://iapp.org/media/pdf/publications/European_Privacy_Chapter_One.pdf, [fecha de consulta: 2 de mayo 2018].

Tribunal de Justicia de la Unión Europea. (2014). *Sentencia del Tribunal de Justicia (Gran Sala) de 13 de mayo de 2014*. Google Inc. vs Agencia Española de Protección de Datos Personales y Mario Costeja González. Disponible en: http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES, [fecha de consulta: 2 de mayo 2018].

# CAPÍTULO II
# DEL EJERCICIO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, CANCELACIÓN Y OPOSICIÓN

***Artículo 48.*** *La recepción y trámite de las solicitudes para el ejercicio de los derechos ARCO que se formulen a los responsables, se sujetará al procedimiento establecido en el presente Título y demás disposiciones que resulten aplicables en la materia.*

***Artículo 49.*** *Para el ejercicio de los derechos ARCO será necesario acreditar la identidad del titular y, en su caso, la identidad y personalidad con la que actúe el representante.*

*El ejercicio de los derechos ARCO por persona distinta a su titular o a su representante, será posible, excepcionalmente, en aquellos supuestos previstos por disposición legal, o en su caso, por mandato judicial.*

*En el ejercicio de los derechos ARCO de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad, de conformidad con las leyes civiles, se estará a las reglas de representación dispuestas en la misma legislación.*

*Tratándose de datos personales concernientes a personas fallecidas, la persona que acredite tener un interés jurídico, de conformidad con las leyes aplicables, podrá ejercer los derechos que le confiere el presente Capítulo, siempre que el titular de los derechos hubiere expresado fehacientemente su voluntad en tal sentido o que exista un mandato judicial para dicho efecto.*

***Artículo 50.*** *El ejercicio de los derechos ARCO deberá ser gratuito. Sólo podrán realizarse cobros para recuperar los costos de reproducción, certificación o envío, conforme a la normatividad que resulte aplicable.*

*Para efectos de acceso a datos personales, las leyes que establezcan los costos de reproducción y certificación deberán considerar en su determinación que los montos permitan o faciliten el ejercicio de este derecho.*

*Cuando el titular proporcione el medio magnético, electrónico o el mecanismo necesario para reproducir los datos personales, los mismos deberán ser entregados sin costo a éste.*

*La información deberá ser entregada sin costo, cuando implique la entrega de no más de veinte hojas simples. Las unidades de transparencia podrán exceptuar el pago de reproducción y envío atendiendo a las circunstancias socioeconómicas del titular.*

*El responsable no podrá establecer para la presentación de las solicitudes del ejercicio de los derechos ARCO algún servicio o medio que implique un costo al titular.*

***Artículo 51.*** *El responsable deberá establecer procedimientos sencillos que permitan el ejercicio de los derechos ARCO, cuyo plazo de respuesta no deberá exceder de veinte días contados a partir del día siguiente a la recepción de la solicitud.*

*El plazo referido en el párrafo anterior podrá ser ampliado por una sola vez hasta por diez días cuando así lo justifiquen las circunstancias, y siempre y cuando se le notifique al titular dentro del plazo de respuesta.*

*En caso de resultar procedente el ejercicio de los derechos ARCO, el responsable deberá hacerlo efectivo en un plazo que no podrá exceder de quince días contados a partir del día siguiente en que se haya notificado la respuesta al titular.*

***Artículo 52.*** *En la solicitud para el ejercicio de los derechos ARCO no podrán imponerse mayores requisitos que los siguientes:*

*I. El nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones;*

*II. Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante;*

*III. De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud;*

*IV. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO, salvo que se trate del derecho de acceso;*

*V. La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular, y*

*VI. Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso.*

*Tratándose de una solicitud de acceso a datos personales, el titular deberá señalar la modalidad en la que prefiere que éstos se reproduzcan. El responsable deberá atender la solicitud en la modalidad requerida por el titular, salvo que exista una imposibilidad física o jurídica que lo limite a reproducir los datos personales en dicha modalidad, en este caso deberá ofrecer otras modalidades de entrega de los datos personales fundando y motivando dicha actuación.*

*En caso de que la solicitud de protección de datos no satisfaga alguno de los requisitos a que se refiere este artículo, y el Instituto o los organismos garantes no cuenten con elementos para subsanarla, se prevendrá al titular de los datos dentro de los cinco días siguientes a la presentación de la solicitud de ejercicio de los derechos ARCO, por una sola ocasión, para que subsane las omisiones dentro de un plazo de diez días contados a partir del día siguiente al de la notificación.*

*Transcurrido el plazo sin desahogar la prevención se tendrá por no presentada la solicitud de ejercicio de los derechos ARCO.*

*La prevención tendrá el efecto de interrumpir el plazo que tiene el Instituto, o en su caso, los organismos garantes, para resolver la solicitud de ejercicio de los derechos ARCO.*

*Con relación a una solicitud de cancelación, el titular deberá señalar las causas que lo motiven a solicitar la supresión de sus datos personales en los archivos, registros o bases de datos del responsable.*

*En el caso de la solicitud de oposición, el titular deberá manifestar las causas legítimas o la situación específica que lo llevan a solicitar el cese en el tratamiento, así como el daño o perjuicio que le causaría la persistencia del tratamiento, o en su caso, las finalidades específicas respecto de las cuales requiere ejercer el derecho de oposición.*

*Las solicitudes para el ejercicio de los derechos ARCO deberán presentarse ante la Unidad de Transparencia del responsable, que el titular considere competente, a través de escrito libre, formatos, medios electrónicos o cualquier otro medio que al efecto establezca el Instituto y los Organismos garantes, en el ámbito de sus respectivas competencias.*

*El responsable deberá dar trámite a toda solicitud para el ejercicio de los derechos ARCO y entregar el acuse de recibo que corresponda.*

*El Instituto y los Organismos garantes, según corresponda, podrán establecer formularios, sistemas y otros métodos simplificados para facilitar a los titulares el ejercicio de los derechos ARCO.*

*Los medios y procedimientos habilitados por el responsable para atender las solicitudes para el ejercicio de los derechos ARCO deberán ser de fácil acceso y con la mayor cobertura posible considerando el perfil de los titulares y la forma en que mantienen contacto cotidiano o común con el responsable.*

***Artículo 53.*** *Cuando el responsable no sea competente para atender la solicitud para el ejercicio de los derechos ARCO, deberá hacer del conocimiento del titular dicha situación dentro de los tres días siguientes a la presentación de la solicitud, y en caso de poderlo determinar, orientarlo hacia el responsable competente.*

*En caso de que el responsable declare inexistencia de los datos personales en sus archivos, registros, sistemas o expediente, dicha declaración deberá constar en una resolución del Comité de Transparencia que confirme la inexistencia de los datos personales.*

*En caso de que el responsable advierta que la solicitud para el ejercicio de los derechos ARCO corresponda a un derecho diferente de los previstos en la presente Ley, deberá reconducir la vía haciéndolo del conocimiento al titular.*

***Artículo 54.*** *Cuando las disposiciones aplicables a determinados tratamientos de datos personales establezcan un trámite o procedimiento específico para solicitar el ejercicio de los derechos ARCO, el responsable deberá informar al titular sobre la existencia del mismo, en un plazo no mayor a cinco días siguientes a la presentación de la solicitud para el ejercicio de los derechos ARCO, a efecto de que este último decida si ejerce sus derechos a través del trámite específico, o bien, por medio del procedimiento que el responsable haya institucionalizado para la atención de solicitudes para el ejercicio de los derechos ARCO conforme a las disposiciones establecidas en este Capítulo.*

***Artículo 55.*** *Las únicas causas en las que el ejercicio de los derechos ARCO no será procedente son:*

*I.* *Cuando el titular o su representante no estén debidamente acreditados para ello;*

*II.* *Cuando los datos personales no se encuentren en posesión del responsable;*

*III.* *Cuando exista un impedimento legal;*

*IV.* *Cuando se lesionen los derechos de un tercero;*

*V.* *Cuando se obstaculicen actuaciones judiciales o administrativas;*

*VI.* *Cuando exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de los mismos;*

*VII.* *Cuando la cancelación u oposición haya sido previamente realizada;*

*VIII.* *Cuando el responsable no sea competente;*

*IX. Cuando sean necesarios para proteger intereses jurídicamente tutelados del titular;*

*X. Cuando sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular;*

*XI. Cuando en función de sus atribuciones legales el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado mexicano, o*

*XII. Cuando los datos personales sean parte de la información que las entidades sujetas a la regulación y supervisión financiera del sujeto obligado hayan proporcionado a éste, en cumplimiento a requerimientos de dicha información sobre sus operaciones, organización y actividades.*

*En todos los casos anteriores, el responsable deberá informar al titular el motivo de su determinación, en el plazo de hasta veinte días a los que se refiere el primer párrafo del artículo 51 de la presente Ley y demás disposiciones aplicables, y por el mismo medio en que se llevó a cabo la solicitud, acompañando, en su caso, las pruebas que resulten pertinentes.*

***Artículo 56.*** *Contra la negativa de dar trámite a toda solicitud para el ejercicio de los derechos ARCO o por falta de respuesta del responsable, procederá la interposición del recurso de revisión a que se refiere el artículo 94 de la presente Ley.*

## COMENTARIO

**Miguel Recio Gayo**

Los derechos ARCO dan a la persona el control sobre el tratamiento de sus datos personales por el responsable y para que pueda ejercerse dicho control es necesario un procedimiento que sea sencillo, ágil y efectivo.

Los comentarios que se hacen a continuación tienen por objeto proporcionar una visión general del procedimiento para el ejercicio de los derechos ARCO, a que se refiere el presente capítulo. Para ello, se hará una referencia a los antecedentes del mencionado procedimiento y algunas consideraciones generales sobre el ejercicio de los derechos ARCO. Asimismo, una aproximación general a dicho procedimiento permitirá centrar algunas cuestiones relevantes para entender su significado, alcance e implicaciones.

El desarrollo del procedimiento para el ejercicio de los derechos ARCO en la LGPDPPSO implica analizar también la legitimación para la presentación de solicitudes, el contenido de dichas solicitudes, así como los plazos aplicables y eventos que podrían darse en la tramitación del procedimiento, las causas de

improcedencia o qué ocurre en los casos de negativa por el responsable del tratamiento a dar trámite a una solicitud o su falta de respuesta.

El análisis del capítulo contempla algunas consideraciones adicionales que, en su caso, pueden servir como referencia para el futuro. Por último, se incluyen también las correspondientes conclusiones.

## I. Antecedentes

Como indicó Patricia Kurczyn Villalobos, comisionada del INAI, durante la audiencia pública en el Senado de la República para plantear sus comentarios, observaciones y propuestas de redacción al primer documento de trabajo sobre el preproyecto de Dictamen de las Comisiones Unidas de Gobernación y de Estudios Legislativos Primera "el derecho de protección de datos deriva, entre otros aspectos, del poder de disposición que tiene toda persona para acceder, rectificar, cancelar u oponerse a un determinado tratamiento de sus datos".[92]

Poder saber qué datos personales trata o no el responsable del tratamiento; rectificar los datos incorrectos o incompletos; instar al responsable a cancelar los datos personales cuando ya no son necesarios para la finalidad o finalidades para las que fueron recabados o cuando su tratamiento es ilícito, u oponerse al tratamiento de datos personales cuando se den determinadas circunstancias relativas al titular de los mismos, deben asegurar a éste un control efectivo, garantizándole así su derecho humano a la protección de datos personales. Es decir, en relación con el derecho humano a la protección de datos personales, estos derechos significan que "el núcleo duro podría establecerse en la potestad de disposición y manejo de la información".[93]

Al respecto, saber qué datos personales trata el responsable o rectificarlos no requiere justificación alguna, tal como se prevé expresamente en la CPEUM. Lo anterior supone una importante diferencia con los derechos de cancelación y oposición, ya que debe entenderse que sí será necesaria algún tipo de justificación para el ejercicio de dichos derechos.

El artículo 6º, apartado A, fracción III, de la CPEUM, indica que "toda persona, sin necesidad de acreditar interés alguno o justificar su utilización,

[92] Senado de la República. (2015). *Dictamen de las Comisiones Unidas de Gobernación y de Estudios Legislativos Primera, con Proyecto de Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados*, p. 17. [Archivo PDF]. Disponible en: http://www.senado.gob.mx/comisiones/gobernacion/docs/proteccion_datos/Documento3.pdf, [fecha de consulta: 3 de mayo 2018].

[93] Magallanes, V. (2016). El derecho a la protección de datos personales. Su diseño constitucional. *Estudios en Derecho a la Información*, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, núm. 2, julio-diciembre, p. 42. Disponible en: https://revistas.juridicas.unam.mx/index.php/derecho-informacion/article/view/10486/12651.

tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos." Es con la reforma constitucional de 2009 cuando se "establece el derecho humano a la protección de los datos personales y sus correlativos derechos de acceso, rectificación, cancelación y oposición, mismos que no sólo harán valer ante las autoridades gubernamentales en cualquiera de sus órdenes de gobierno, sino, además, ante los propios particulares que se encuentren en posesión de datos personales".[94]

La LGPDPPSO incluye, además de otros derechos en protección de datos personales, los derechos ARCO, lo que supone ampliar los derechos que ya se preveían en la abrogada Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG). Sobre esta cuestión, Maqueo y Moreno apuntan que "la citada Ley sólo contemplaba, de manera tímida, los derechos de acceso y rectificación de datos personales sin incluir los de oposición y cancelación del titular de los mismos".[95]

En cuanto al derecho de acceso, el artículo 24 de la LFTAIPG indicaba que "sólo los interesados o sus representantes podrán solicitar a una unidad de enlace o su equivalente, previa acreditación, que les proporcione los datos personales que obren en un sistema de datos personales".

Y por lo que se refiere al derecho de rectificación, el artículo 25 de la LFTAIPG indicaba en lo sustancial que "las personas interesadas o sus representantes podrán solicitar, previa acreditación, ante la unidad de enlace o su equivalente, que modifiquen sus datos que obren en cualquier sistema de datos personales".

El ejercicio de ambos derechos se sustentaba sobre las obligaciones del responsable del tratamiento previstas, respectivamente, en las fracciones I y V del artículo 20 de la LFTAIPG. La fracción I, relativa a los procedimientos de acceso y corrección de los datos personales, indicaba que, como responsables de los datos personales, los sujetos obligados deberán "adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos". Y la fracción V, relativa al derecho de rectificación, indicaba que el responsable del tratamiento tenía obligación de "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".

---

[94] Maqueo, M. y Moreno, J. (2014). *Implicaciones de una ley general en materia de protección de datos*, Documento de Trabajo núm. 64, División de Estudios Jurídicos del Centro de Investigación y Docencia Económicas, p. 8. [Archivo PDF]. Disponible en: http://www.libreriacide.com/librospdf/DTEJ-64.pdf, [fecha de consulta: 3 de mayo 2018].

[95] *Ibíd.*, p. 7.

En desarrollo de lo previsto en la LFTAIPG se publicaron los Lineamientos de Protección de Datos Personales,[96] en cuya introducción se resalta la importancia de que "las personas tengan conocimiento de la información que de ellos obra en los archivos del Gobierno Federal a efecto de hacer uso del derecho de acceso y corrección de los datos personales que les conciernen, así como de conocer las transferencias de sistemas de datos personales efectuadas para el cumplimiento de las atribuciones de las unidades administrativas que lo conforman". Y lo anterior dio lugar a la aplicación informática denominada Sistema Persona.

Para que el titular pueda controlar el uso de sus datos personales e instar al responsable del tratamiento a cumplir con su obligación de garantizar los derechos del afectado, como se indica en el Lineamiento primero, se incluye también, en el Lineamiento octavo, la obligación de que los datos personales se almacenen en los sistemas de información "de forma tal que permitan el ejercicio de los derechos de acceso y corrección previstos por la Ley, el Reglamento y los Lineamientos emitidos por el Instituto".

El ejercicio de los derechos ARCO tiene que facilitarse por medio de un procedimiento sencillo, ya que lo contrario podría suponer un obstáculo que, al impedir o dificultar dicho ejercicio, vulnerase el derecho humano a la protección de datos personales. En concreto, la LGPDPPSO indica, en su artículo 52, que "los medios y procedimientos habilitados por el responsable para atender las solicitudes para el ejercicio de los derechos ARCO deberán ser de fácil acceso y con la mayor cobertura posible considerando el perfil de los titulares". Por tanto, el responsable tendrá que adoptar e implementar un procedimiento que cumpla con estas características, garantizando el fácil ejercicio de los derechos ARCO a todos los titulares de los datos, así como su derecho humano a la protección de datos personales.

Para completar los antecedentes cabe hacer una referencia al ámbito internacional. En donde debe atenderse, por una parte, al Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal[97] y por otra parte, tanto a la Directiva 95/46/CE[98] como al Reglamento General de Protección de Datos (RGPD).[99]

---

[96] Disponible en: http://inicio.inai.org.mx/MarcoNormativoDocumentos/lineamientos_protdaper.pdf

[97] Disponible en: https://rm.coe.int/16806c1abd.

[98] 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, *Diario Oficial de las Comunidades Europeas,* L 281, el 23 de noviembre de 1995.

[99] 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), *Diario Oficial de la Unión Europea,* L 119, el 4 de mayo de 2016.

El Convenio 108 del Consejo de Europa incluye los derechos de acceso, rectificación y cancelación en las letras b) y c) del artículo 8, refiriéndose al contenido de los mismos. La Directiva 95/46/CE (que no se aplica desde el 24 de mayo de 2018 ya que queda derogada a partir del 25 de mayo de 2018) establecía en su artículo 12 los derechos de acceso, rectificación y supresión o bloqueo. Y el RGPD de la UE amplía el listado de derechos, incluyendo nuevos, como el derecho a la portabilidad o a la limitación del tratamiento, a los que dedica el Capítulo III, artículos 12 a 23.

En particular, el RGPD establece en sus considerandos, que sirven para interpretar también sus artículos, que los responsables del tratamiento deben implementar "fórmulas para facilitar al interesado el ejercicio de sus derechos" (Considerando 59) y también que "el responsable del tratamiento también debe proporcionar medios para que las solicitudes se presenten por medios electrónicos, en particular cuando los datos personales se tratan por medios electrónicos." Finalmente, el mencionado considerando indica que "el responsable del tratamiento debe estar obligado a responder a las solicitudes del interesado sin dilación indebida y a más tardar en el plazo de un mes, y a explicar sus motivos en caso de que no fuera a atenderlas".

## II. Análisis del contenido

**1. Aproximación al procedimiento para el ejercicio de los derechos ARCO.** La LGPDPPSO establece los elementos y los criterios a considerar en la implementación y aplicación del procedimiento para el ejercicio de los derechos ARCO. Se incluye también en el articulado del capítulo la lista cerrada de causas que determinan la improcedencia de las solicitudes para el ejercicio de los derechos, sin perjuicio de que ninguno de los mencionados derechos sea absoluto, aunque esto último es una cuestión relativa al contenido y alcance de los mismos.

Tanto para hacer efectivos cada uno de los derechos ARCO como para garantizar también que el responsable del tratamiento cumpla con los principios de la protección de datos personales, el procedimiento para el ejercicio de los derechos ARCO es un mecanismo esencial. Saber si un responsable trata o no los datos personales por medio del derecho de acceso o si los datos se mantienen actualizados en virtud del derecho de cancelación, requiere de un procedimiento que los haga efectivos, de manera sencilla y sin dilaciones.

En cuanto a su alcance, como cualquier otro procedimiento, el objetivo del procedimiento para el ejercicio de los derechos ARCO es establecer la forma específica en que se atenderán, lo que implica desde la recepción de la solicitud hasta la respuesta que se dará al titular de los datos personales o cualquier otro evento que se produzca como, por ejemplo, la necesidad de subsanación de la solicitud por el titular de los datos personales.

El procedimiento para el ejercicio de los derechos ARCO, aquí previsto, es el que podría denominare como general, ya que en caso de que hubiera otras disposiciones aplicables al tratamiento de datos en las que se establezca un trámite o procedimiento específico, como indica el artículo 54 de la LGPDPPSO, el responsable del tratamiento "deberá informar al titular sobre la existencia del mismo". No obstante, el citado artículo, a continuación, indica también que será el titular de los datos quien decidirá "si ejerce sus derechos por medio del trámite específico, o bien, por medio del procedimiento que el responsable haya institucionalizado" conforme a lo dispuesto en la propia ley.

Sobre el procedimiento específico, en la *Guía para Titulares de Datos Personales*, el INAI destaca que "el responsable deberá informar al titular sobre la existencia de dicho trámite o procedimiento en un plazo máximo de 5 días hábiles contados a partir del día siguiente de la presentación de la solicitud".[100]

Es decir, salvo que haya un procedimiento específico y el titular de los datos personales decida recurrir al mismo, se deberá atender al procedimiento para el ejercicio de derechos ARCO que el responsable del tratamiento implemente en virtud de la LGPDPPSO. Y, en cualquier caso, el procedimiento específico deberá facilitar que los titulares de los datos personales puedan ejercer sus derechos ARCO con iguales garantías que las previstas en la LGPDPPSO. En este sentido, lo anterior queda fundamentado tanto en la Disposición Transitoria Cuarta, en virtud de la que "se derogan todas aquellas disposiciones en materia de protección de datos personales de carácter federal, estatal y municipal que contravengan lo dispuesto por la presente ley", como en la Disposición Transitoria Octava que establece que "no se podrán reducir o ampliar en la normatividad de las entidades federativas, los procedimientos y los plazos vigentes aplicables en la materia, en perjuicio de los titulares de datos personales".

En relación con este procedimiento es necesario tener en consideración que la LGPDPPSO señala, por una parte, que "el responsable deberá establecer procedimientos sencillos que permitan el ejercicio de los derechos ARCO" y, por otra, que la solicitud deberá ser contestada en un plazo máximo previsto en la misma, que es de veinte días hábiles, prorrogables por un plazo único de diez días hábiles "cuando así lo justifiquen las circunstancias, y siempre y cuando se le notifique al titular", como indica el artículo 51.

Además, este procedimiento es gratuito (artículo 50 de la LGPDPPSO), sin perjuicio de que puedan realizarse "cobros para reproducir los datos personales" y en aquellos casos en los que la entrega de los datos implique "más

[100] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2017). *Guía para Titulares de los Datos Personales*, vol. 3. México: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, p. 14.

de veinte hojas simples". Que el procedimiento sea gratuito conlleva también que, como se establece en el último párrafo del artículo 50 de la LGPDPPSO, el responsable del tratamiento "no podrá establecer para la presentación de las solicitudes de ejercicio de los derechos ARCO algún servicio o medio que implique un costo al titular", de manera que los números de tarificación especial u otros medios similares que impliquen un costo adicional supondrían un incumplimiento y, por tanto, un obstáculo al ejercicio de los derechos ARCO.

Siempre que cumpla con los objetivos y las garantías previstas en el capítulo relativo al ejercicio de los derechos ARCO, cada responsable del tratamiento podrá establecer el procedimiento que estime oportuno, ya sea electrónico u otro mecanismo o ambos simultáneamente, facilitando así que los titulares de los datos personales puedan solicitar por cualquier vía el ejercicio de sus derechos.

El procedimiento para el ejercicio de los derechos ARCO debe ser ágil, sencillo y efectivo, lo cual se podrá conseguir por medio de las medidas previstas en el articulado del capítulo relativo a dicho procedimiento en la LGPDPPSO. Esto implica que cualquier regulación o disposición sobre el procedimiento para el ejercicio de los derechos ARCO centre su atención en garantizar el derecho humano a la protección de datos a través de requisitos claros y que el responsable del tratamiento pueda aplicar, en virtud de las circunstancias específicas, ahora y en el futuro.

En concreto, los artículos de este capítulo están dedicados a quienes están legitimados para ejercerlos, ya que, si bien es un derecho personal se prevén diferentes supuestos como el carácter gratuito (sin perjuicio de los costos previstos en ciertos casos específicos); los plazos aplicables en la tramitación de las solicitudes para el ejercicio de los derechos ARCO; el contenido de la solicitud y los criterios a considerar para su presentación y tramitación; las causas de improcedencia y las consecuencias de la negativa por el responsable del tratamiento o dar trámite a la solicitud o la falta de respuesta a la misma.

**2. Legitimación para la presentación de solicitudes.** La legitimación para el ejercicio de los derechos ARCO es una de las cuestiones relevantes del procedimiento, ya que cuando el responsable del tratamiento recibe una solicitud, comprobar si la persona que la presenta está legitimada para ello es la primera cuestión a la que se debe atender.

La LGPDPPSO, en su artículo 49, incluye los diferentes casos de legitimación en la solicitud para el ejercicio de los derechos, que son los relativos a:

1. El titular de los datos o su representante legal. Aquí se incluyen también los casos de menores y personas que se encuentren en estado de interdicción o incapacidad.

2. Persona distinta al titular de los datos o su representante legal, siendo una situación excepcional y en la que será necesario atender a los "supuestos previstos por disposición legal, o en su caso, por mandato judicial".
3. Personas fallecidas, en cuyo caso quien ejercerá el derecho será "la persona que acredite tener un interés jurídico" y "siempre que el titular de los derechos hubiera expresado fehacientemente su voluntad en tal sentido o que exista un mandamiento judicial para dicho efecto".

En relación con este último caso, el relativo al ejercicio de derechos ARCO de personas fallecidas, cabría plantear que se trata de un supuesto excepcional que requerirá de interpretación en la práctica. A diferencia de otros casos no hay un titular de los datos que vaya a obtener el resultado del ejercicio de sus derechos, porque la persona a la que se refieren ha fallecido, lo que implica que dejó de ser aplicable la normatividad sobre protección de datos. Por lo tanto, más que ejercer un derecho, lo que se produciría es la comunicación al responsable del tratamiento sobre el fallecimiento del titular de los datos personales para que proceda a adoptar las medidas oportunas, tales como la cancelación.

Si no fuera así, habría que considerar si se trata de un caso diferente en el que una persona distinta al titular de los datos, cuando se cumplan las condiciones previstas relativas a que el fallecido hubiera "expresado fehacientemente su voluntad" o bien que "exista un mandato judicial", pueda, por ejemplo, acceder a datos personales del expediente clínico de quien ya ha fallecido para saber si una enfermedad es hereditaria o no.

**3. Contenido de la solicitud para el ejercicio de derechos.** Como parte del procedimiento, la LGPDPPSO incluye también cuál es el contenido de la solicitud que se presenta al responsable del tratamiento para el ejercicio de los derechos ARCO.

Sobre los requisitos aplicables a la solicitud es necesario atender al artículo 52 de la LGPDPPSO "no podrán imponerse mayores requisitos" lo que implica, por una parte, que el responsable no podrá exigir requisitos adicionales y, por otra parte, que los aquí previstos deban tomarse en cuenta en el caso de que existiera un procedimiento específico previsto en la normatividad o disposiciones aplicables, ya que de otra manera podría vulnerarse el derecho humano a la protección de datos personales. Es decir, en el caso de que hubiera un procedimiento en virtud de las disposiciones específicas, el contenido de la solicitud sólo podrá ser distinto al indicado en la LGPDPPSO si hay motivos fundamentados para ello, ya que en otro caso, supondría una divergencia injustificada.

En concreto, los requisitos aplicables a la solicitud para el ejercicio de los derechos ARCO se refieren a los siguientes elementos:

**Tabla 3. Requisitos aplicables a la solicitud para el ejercicio de los derechos ARCO**

| Elemento(s) | Requisito(s) |
|---|---|
| Identidad del titular y datos de contacto a efectos de notificaciones | El nombre del titular y su domicilio o cualquier otro medio para recibir notificaciones (fracción I). |
| | Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante (fracción II). |
| Presentación de la solicitud al responsable del tratamiento | De ser posible, el área responsable que trata los datos personales y ante el cual se presenta la solicitud (fracción III). |
| Derecho(s) ARCO que se ejercita(n) | La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos ARCO, salvo que se trate del derecho de acceso (fracción IV). |
| | La descripción del derecho ARCO que se pretende ejercer, o bien, lo que solicita el titular (fracción V). |
| | Cualquier otro elemento o documento que facilite la localización de los datos personales, en su caso (fracción VI). |

Sin perjuicio de lo anterior, el mencionado artículo indica también que, en el caso del derecho de acceso a datos personales, será el titular quien elija "la modalidad en la que prefiere que éstos se reproduzcan" por medio de su solicitud.

En caso de que la modalidad de reproducción de los datos elegida por el titular de los mismos no sea posible debido a que "exista una imposibilidad física o jurídica que lo limite", el responsable del tratamiento deberá ofrecer otras modalidades de entrega fundamentando y motivando dicha actuación. No obstante, la modalidad de entrega que el responsable pudiera ofrecer deberá permitir siempre que el titular pueda tener acceso a sus datos personales, ya que de no ser así se impediría su ejercicio.

**4. Plazos aplicables a considerar en la tramitación de solicitudes.** Otra cuestión igualmente relevante en cuanto al ejercicio de los derechos ARCO es la relativa a los plazos aplicables a la solicitud que efectúe el titular de los datos personales. Tanto el responsable del tratamiento como el titular de los datos personales tienen que considerar los diversos plazos que se indican a lo largo de los artículos que componen el presente capítulo. Se trata de plazos dispersos a lo largo del articulado a los que hay que atender para garantizar el derecho humano a la protección de datos personales.

Cuando el responsable del tratamiento recibe una solicitud para el ejercicio de derechos ARCO, debe atender a los diferentes eventos y plazos previstos y que son los que se indican a continuación:

**Tabla 4. Relación de eventos y plazos previstos, que el responsable debe considerar para el ejercicio de derechos ARCO**

| Evento o acción | Plazo | Cómputo del plazo |
|---|---|---|
| Respuesta a la solicitud para el ejercicio de derechos ARCO y notificación al titular | Máximo veinte (20) días. | A partir del día siguiente a la recepción de la solicitud. |
| | Posibilidad de ampliación por una sola vez hasta por diez (10) días si las circunstancias lo justifican y se notifica al titular dentro del plazo de respuesta. | |
| Hacer del conocimiento del titular de los datos que el responsable no es competente para atender la solicitud para el ejercicio de derechos ARCO | Máximo tres (3) días. | |
| Prevenir al titular de los datos para que subsane la falta de alguno de los requisitos indicados en el artículo 52 de la LGPDPPSO | Máximo cinco (5) días. | |
| Informar al titular de los datos sobre la existencia de un trámite o procedimiento específico para el ejercicio de los derechos ARCO en virtud de disposiciones aplicables al tratamiento específico que se haga | Máximo cinco (5) días. | |
| Informar al titular de los datos personales de la improcedencia del ejercicio de los derechos ARCO | Máximo veinte (20) días. | |
| Hacer efectivo el ejercicio de los derechos ARCO cuando la solicitud es procedente | Máximo quince (15) días. | A partir del día siguiente en que se notifique la respuesta al titular. |

Los días a los que se hace referencia son días hábiles. Por otra parte, el titular de los datos personales deberá tener en consideración que en caso de que se le requiera subsanar la solicitud para el ejercicio de los derechos ARCO, debido a la falta de alguno de los requisitos indicados en el artículo 52 de la LGPDPPSO, tendrá que hacerlo dentro del plazo de diez (10) días a partir del día siguiente a que se le notifique. Si el titular no subsana su solicitud en el plazo mencionado, se tendrá por no presentada.

**5. Causas de improcedencia, consecuencias de la negativa a dar trámite y de la falta de respuesta a las solicitudes.** La LGPDPPSO contempla tres casos en los que la solicitud para el ejercicio de los derechos ARCO: a) será improcedente por concurrir alguno de los motivos que se exponen a continuación; b) no se le da trámite por el responsable del tratamiento, o c) queda sin respuesta.

En el artículo 55 de la LGPDPPSO se incluye una lista exhaustiva de causas "en la que el ejercicio de los derechos ARCO no será procedente". Dichas causas responden a diferentes criterios, que podrían ser los que se indican a continuación y que permiten agruparlas de la siguiente manera:

**Tabla 5. Criterios y causales de improcedencia del ejercicio de los derechos ARCO**

| Criterio o motivo a considerar | Causal de improcedencia del ejercicio de los derechos ARCO |
|---|---|
| Relativo al propio titular de los datos personales | Cuando el titular o su representante no estén debidamente acreditados para ello (fracción I). |
| | Cuando sean necesarios para proteger intereses jurídicamente tutelados del titular (fracción IX). |
| | Cuando sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por el titular (fracción X). |
| Relativo a los datos personales | Cuando los datos personales no se encuentren en posesión del responsable (fracción II). |
| Relativos a límites derivados de previsiones legales, ejercicio de funciones judiciales o administrativas, resoluciones, derechos de terceros o seguridad nacional | Cuando exista un impedimento legal (fracción III). |
| | Cuando se lesionen los derechos de un tercero (fracción IV). |
| | Cuando se obstaculicen actuaciones judiciales o administrativas (fracción V). |
| | Cuando exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de los mismos (fracción VI). |
| | Cuando en función de sus atribuciones legales o el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado mexicano (fracción XI). |
| Derivados de información ya proporcionada o ejercicio previo de los derechos | Cuando los datos personales sean parte de la información que las entidades sujetas a la regulación y supervisión financiera del sujeto obligado hayan proporcionado a éste, en cumplimiento a requerimientos de dicha información sobre sus operaciones, organización y actividades (fracción XII). |
| | Cuando la cancelación u oposición haya sido previamente realizada (fracción VII). |
| Relativo al responsable del tratamiento | Cuando el responsable no sea competente (fracción VIII). |

En comparación con la LFPDPPP, algunas de las causas de improcedencia de las solicitudes para el ejercicio de los derechos ARCO se encuentran también aquí previstas y a las mismas se han agregado otras específicas aplicables en el sector público.

Por lo que se refiere a los demás casos, tanto cuando se produce negativa por el responsable del tratamiento a dar trámite a una solicitud para el ejercicio de los derechos ARCO como cuando hay falta de respuesta, una vez transcurrido el plazo de respuesta, el titular de los datos podrá imponer el correspondiente recurso de revisión.

**6. Consideraciones adicionales.** En cuanto a la tramitación de la solicitud para el ejercicio de los derechos ARCO, cabe resaltar que la LGPDPPSO indica, en el artículo 52, que el responsable tiene la obligación de dar trámite a toda solicitud que reciba entregando el correspondiente acuse de recibo al titular de los datos y que las solicitudes "deberán presentarse ante la Unidad de Transparencia del responsable, que el titular considere competente". También incluye como una de las causas de improcedencia la relativa a que "los datos personales no se encuentren en posesión del responsable", como indica la fracción II del artículo 55.

Al respecto, en cualquier caso, debe quedar claro que si la persona que recibe la solicitud para el ejercicio de los derechos ARCO trata los datos personales o no, deberá contestar en uno u otro sentido, ya que el hecho de no tratar datos personales es también parte del ejercicio del derecho de acceso. Es decir, el derecho de acceso permite saber al titular si a quien se dirige la solicitud trata o no sus datos personales, de esta forma, se convierte también en un instrumento para ejercer los demás derechos, ya sean los de rectificación, cancelación y oposición u otros.

El hecho de que los datos personales no se encuentren en posesión del responsable, más que una causal de improcedencia implicaría que el responsable del tratamiento tenga que responder que no trata datos personales del titular. Es decir, el derecho de acceso deberá permitir al titular de los datos saber si el responsable al que dirige su solicitud trata o no sus datos personales y, en su caso, poder ejercer otros derechos. Y en caso de que no los trate, tendrá que declarar su inexistencia conforme a lo previsto en la LGPDPPSO, de manera que el Comité de Transparencia deberá confirmar la resolución.

Por último, más allá de que el titular de los datos pueda proporcionar el medio magnético, electrónico o mecanismo necesario para reproducir los datos personales, se podría considerar un impulso decidido del uso de las tecnologías de la información y las comunicaciones para facilitar el ejercicio de los derechos ARCO, incluyendo también el de rectificación, por ejemplo, en el área del usuario al que pueda acceder para consultar y, en su caso, rectificar sus datos personales. Lo anterior, unido al uso de medios de identificación electrónica previstos en la normatividad, tales como la firma electrónica, deberán ser aprovechados para hacer efectivo el ejercicio de los derechos ARCO.

## III. Conclusiones

En virtud de las consideraciones hechas previamente, es posible presentar las siguientes conclusiones:

Primera.- Los artículos 48 al 56 del Capítulo II Del Ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición, correspondiente al Título Tercero Derechos de los Titulares y su Ejercicio, tienen por objeto establecer el procedimiento para el ejercicio de los derechos ARCO por medio del que el responsable del tratamiento deberá recibir y tramitar toda solicitud al respecto.

Segunda.- Con respecto a la abrogada LFTAIPG de 2002, la LGPDPPSO incluye los derechos de cancelación y oposición, además de los de acceso y rectificación.

Tercera.- El procedimiento para el ejercicio de los derechos ARCO tiene que ser sencillo para el titular de los datos personales, ágil en cuanto a los tiempos de respuesta, de manera que no se produzcan dilaciones, y efectivo. Se trata así de garantizar al titular de los datos su derecho humano a la protección de datos personales.

Cuarta.- En relación con dicho procedimiento, la LGPDPPSO incluye disposiciones relativas a la legitimación para la presentación de la solicitud correspondiente, los plazos que habrán de considerarse tanto por el responsable del tratamiento como por el titular de los datos personales en relación con la tramitación de la solicitud presentada, las causas de improcedencia y las consecuencias de la negativa por el responsable a dar trámite a una solicitud o su falta de respuesta.

Quinta.- Si hubiera un procedimiento específico para el ejercicio de los derechos ARCO aplicable a determinados datos personales, el responsable del tratamiento tendrá que informar de ello al titular de los datos para que pueda elegir entre ese o por medio del procedimiento institucionalizado por el responsable del tratamiento.

Sexta.- Aunque se prevé el uso de medios magnéticos, electrónicos u otros mecanismos para la reproducción de los datos personales, se debería considerar el uso de las tecnologías de la información y la comunicación en todos los casos y especialmente para el ejercicio de los derechos de acceso y rectificación, siempre que se pueda identificar al titular por medios electrónicos y, si fuera necesario, hacer uso de la firma electrónica para la cumplimentación y envío de solicitudes.

## Referencias

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, publicada en el *Diario Oficial de las Comunidades Europeas,* L 281, el 23 de noviembre de 1995.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2017). *Guía para Titulares de los Datos Personales*, vol. 3. México: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, p.14.

Magallanes, V. (2016). El derecho a la protección de datos personales. Su diseño constitucional. *Estudios en Derecho a la Información*, Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, núm. 2, julio-diciembre, p. 42. Disponible en: https://revistas.juridicas.unam.mx/index.php/derecho-informacion/article/view/10486/12651.

Maqueo, M. y Moreno, J. (2014). *Implicaciones de una ley general en materia de protección de datos*, Documento de Trabajo núm. 64, División de Estudios Jurídicos del Centro de Investigación y Docencia Económicas, p. 8. [Archivo PDF]. Disponible en: http://www.libreriacide.com/librospdf/DTEJ-64.pdf, [fecha de consulta: 3 de mayo 2018].

Senado de la República. (2015). *Dictamen de las Comisiones Unidas de Gobernación y de Estudios Legislativos Primera, con Proyecto de Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados*. [Archivo PDF]. Disponible en: http://www.senado.gob.mx/comisiones/gobernacion/docs/proteccion_datos/Documento3.pdf, [fecha de consulta: 3 de mayo 2018].

# CAPÍTULO III
# DE LA PORTABILIDAD DE LOS DATOS

***Artículo 57.*** *Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.*

*Cuando el titular haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales.*

*El Sistema Nacional establecerá mediante lineamientos los parámetros a considerar para determinar los supuestos en los que se está en presencia de un formato estructurado y comúnmente utilizado, así como las normas técnicas, modalidades y procedimientos para la transferencia de datos personales.*

## COMENTARIO

**Oscar R. Puccinelli**

### I. Antecedentes

La portabilidad, conceptualmente, constituye una respuesta técnica a la necesidad humana de “llevar consigo” ciertos bienes que le son de utilidad y es un concepto clave en la evolución tecnológica, especialmente en el ámbito de las TIC. Históricamente, a cada nueva invención útil la sucedió, invariablemente, alguna versión portátil o portable. Relojes (inicialmente ubicados en edificios públicos), calculadoras (que en sus primeras versiones tenían el tamaño de una

habitación), radios y televisores (ubicados antaño en las salas de estar para servir de esparcimiento familiar), reproductores en general y teléfonos son algunos claros ejemplos de tal proceso. Más recientemente, en la era informática, distintas invenciones redujeron los tamaños y ampliaron las prestaciones de diversos aparatos, convirtiéndose en laptops, tablets, ipods, smartphones, y demás *wearables* o dispositivos de la "tecnología para llevar puesta", generando ahora portabilidades tanto del tiempo como del espacio (de ocio, de trabajo, etc.).

Entre esas portabilidades se instaló, en la era preinformática, la de la información, que estrictamente se inició con la invención de la escritura y se potenció mucho después, primero con la aparición de la imprenta y luego con diversas formas de automatización (mecánica y electrónica) hasta llegar al actual escenario, donde la mayor parte de la información disponible en el mundo se encuentra alojada en una internet participativa, donde todos aportan información (especialmente a través de las redes sociales), y que se hace todavía más compleja a partir de los datos masivos (*big data*), la inteligencia artificial (*AI*), la computación en la nube (*cloud computing*) y la Internet de las cosas (*IoT*), que caracterizan una red en tránsito de una web de las cosas (*web of things*) a una web de los pensamientos (*web of thoughts*), que tipificará a la ya denominada web 4.0.

En el actual contexto tecnológico, la idea de la portabilidad de la información —como fenómeno y como derecho— aparece como una respuesta (ora altruista, ora egoísta) al surgimiento de necesidades humanas que encontraban óbices tanto técnicos —la existencia de formatos heterogéneos e incompatibles de tratamiento de esa información, que dificultan (adrede o no) esa tarea— como jurídicos, por la falta de reconocimiento de un derecho específico a que los datos sean tratados en formatos que permitan esa portabilidad (a la par de la interoperabilidad de los sistemas, otro concepto clave de la evolución tecnológica).

Desde el punto de vista jurídico, en el caso de la información personal, resulta inevitable relacionar como primer antecedente del derecho a la portabilidad al derecho de acceso a los datos personales (de hecho algunos autores refieren, no sin alguna razón, al derecho a la portabilidad como una suerte de *derecho de acceso premium*), el cual, desde su inclusión en el artículo 129 de la Constitución de Weimar de 1919, ha ido adaptándose a los avances tecnológicos (ver, v.gr., el artículo 14 de la Ley Orgánica de Regulación y Tratamiento Automatizado de Datos (LORTAD) española de 1992 y su reglamento, donde se reconocía al interesado el derecho a recibir la información por diferentes medios, aunque esa libertad de elección quedaba supeditada finalmente a la configuración o implantación material del fichero o de la naturaleza del tratamiento).[101]

[101] Allí se reconocía el derecho de recibir la información a través de uno o varios sistemas de consulta: visualización en pantalla; escrito, copia o fotocopia remitida por correo, certificado o no; telecopia; correo electrónico u otros sistemas de comunicaciones electrónicas; o cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable.

Más recientemente, a partir de la mutación de la web a su versión 2.0 (una web participativa caracterizada por la aparición de las redes sociales y la incorporación de los usuarios como nuevos aportantes de información) se torna más patente esa idea —y necesidad— de uniformar los formatos de tratamiento, abriendo paso a la configuración de un derecho que le permitiera al titular de los datos recuperar el control sobre la información que había facilitado a un determinado prestador de servicios de la sociedad de la información en el curso de su relación, facilitándole "llevárselos" en formatos que le permitieran su reutilización, ora en sus sistemas, ora en los de otros prestadores. Así, en 2007 emergerá el *Data Portability Project*, motorizado por un grupo de expertos y decisores del sector de nuevas tecnologías estadounidense, sirviendo como punto de encuentro y foro entre compañías del sector digital para impulsar prácticas de portabilidad homogéneas, sencillas y transparentes para el usuario.

Casi paralelamente, en el ámbito europeo se advirtió la necesidad de reconocer nuevos derechos, entre ellos un remozado derecho *al olvido o a ser olvidado*[102] y el derecho *a la portabilidad de los datos*.[103] En efecto, tomando especialmente en cuenta el impacto benéfico que podría causar reconocer tanto el *derecho a la portabilidad* como el *derecho al olvido* en el caso de los datos proporcionados por niños, niñas y adolescentes en las redes sociales, se comenzó a plantear la idea de la portabilidad de los datos como una suerte de nueva versión de la *portabilidad numérica* incorporada en el ámbito de la telefonía fija y móvil.[104]

En este orden de ideas, Viviane Reding, siendo por entonces Comisaria Europea de Sociedad de la Información y Medios de Comunicación y compartiendo ciertas ideas expuestas por Viktor Mayer-Schönberger respecto a la necesidad de reconocer ciertas formas de olvido en la era digital,[105] en una conferencia brindada en 2010 expresó: "Necesitamos encontrar maneras de potenciar a los internautas. Los usuarios de internet deben sentir que sus derechos fundamentales, y sus datos personales, son seguros en el mundo digital. Los usuarios de internet deben tener un control efectivo de lo que ponen en línea y poder corregirlos, retirarlos o eliminarlos cuando lo deseen. En la reciente consulta pública sobre la revisión de las reglas de protección de datos, nos dijeron que debería haber 'un derecho a ser olvidado'. Tenemos que mirar más de cerca esta idea. Más control también significa poder mover sus datos

[102] *Right to be forgotten* o RTBF, anteriormente aplicado a diversos medios de expresión y ahora ampliado a las informaciones contenidas en la web y conocido como RTBF 2.0.

[103] *Right to data portability*, que también se exhibe en su versión 2.0, a partir de aquella primitiva versión contenida en el derecho de acceso reconocido en la LORTAD española.

[104] La portabilidad numérica fue reconocida primeramente en Hong Kong en 1999, y luego, en el caso europeo, por las directivas 2002/19/CE, 2002/20/CE, 2002/21/CE, 2002/22/ CE del Parlamento Europeo y del Consejo, todas de 07/03/02 (Directivas de acceso, autorizaciones, marco y de servicio universal, transpuestas por ejemplo en España mediante el Real Decreto 2296/2004).

[105] Mayer–Schönberger, V. (2009). *Delete: the virtue of forgetting in the digital age*. EE.UU.: Princeton University Press.

de un lugar a otro, y tenerlos correctamente eliminados de la primera ubicación en el proceso. Si tengo mis preciosas fotos almacenadas en algún lugar de la nube, ¿qué pasa si quiero cambiar a otro proveedor? También hay un importante punto de competencia aquí. Como comisario de telecomunicaciones de la UE, luché para que la portabilidad numérica fuera una opción real para los consumidores, en aras de la competencia. Puedo ver la misma lógica que se aplica aquí con los datos".[106]

Tal punto de vista fue luego recogido en una Comunicación de 2010 de la Comisión Europea en la cual se presentó un diagnóstico sobre la protección de los datos personales en la Unión, enfatizando la necesidad de proteger mejor la privacidad de los niños en la red; reforzar el principio de minimización de datos, mejorar las modalidades de ejercicio de los derechos de acceso, rectificación, borrado o bloqueo de datos, y reconocer explícitamente tanto el derecho al olvido como el derecho a la portabilidad de los datos, por el cual se confiera a la persona concernida "el derecho explícito a retirar sus datos (por ejemplo, fotografías o listas de amigos) de una aplicación o de un servicio, de modo que los datos retirados puedan transferirse a otra aplicación u otro servicio, siempre que ello sea técnicamente posible, sin que los responsables del tratamiento lo obstaculicen".[107]

Poco tiempo más tarde, en otra Comunicación de la Comisión Europea de 2010 donde se abordaba la problemática de la protección de la privacidad en un mundo interconectado y se pretendía aprobar un nuevo marco europeo de protección de datos para el siglo XXI, se presentaron dos iniciativas legislativas: el Reglamento General de Protección de Datos y una directiva sobre el tratamiento de datos personales relativos a infracciones penales, por medio de las cuales se pretendía adecuar el marco normativo existente debido a que éste, en opinión de la Comisión, ya no era suficientemente eficaz para preservar el derecho a la protección de datos personales en el "nuevo y complejo entorno digital actual".

Entre ambas iniciativas, el proyecto de Reglamento General de Protección de Datos (RGPD) contenía diversas innovaciones, entre las cuales se reconocían los derechos al olvido y a la portabilidad. La propuesta generó ese mismo año una reunión interparlamentaria de comisiones en el Parlamento Europeo, a instancias de la Comisión del Parlamento Europeo de Libertades Civiles, Justicia y Asuntos de Interior (LIBE) y la Unidad de Diálogo Legislativo (UDL), donde se trataron aspectos de la implementación práctica del derecho a la portabilidad, aunque

[106] Reding, V. (2010). *Building trust in Europe's online single market*. Brussels: American Chamber of Commerce to the EU. Bruselas. Disponible en: http://europa.eu/rapid/press-release_SPEECH-10-327_en.htm.

[107] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. (2010). *Un enfoque global de la protección de los datos personales en la Unión Europea*. Bruselas.

considerando todavía que el derecho a la portabilidad era una mera variante del derecho de acceso , y por ello el propio Parlamento Europeo fusionó a ambos en el derecho de acceso en la revisión de la Propuesta de Reglamento realizada en 2014, y recién recuperó su autonomía —aunque con ciertos matices respecto de la propuesta original— a partir del Planteamiento General del Consejo de la Unión Europea sobre el RGPD de 2015.

En efecto, hubo diversas reformas respecto del originario artículo 18, por el cual se concedía al interesado, bajo ciertas condiciones, las facultades de: a) obtener una copia de sus datos personales en un formato electrónico estructurado y de uso habitual y b) transferir sus datos, y otras informaciones que haya facilitado, de un sistema de tratamiento electrónico a otro, puesto que: a) se simplificaba su redacción; b) pasaba a entenderse como la facultad de recibir los datos personales en un formato estructurado, de uso común y "capaz de ser leído por una máquina"; c) se evitaba distinguir condicionantes para el ejercicio de las distintas vertientes del derecho (es decir, tanto la facultad del interesado para solicitar una copia de sus datos como la de solicitar al responsable el traslado de los datos a otro sistema pasaría a depender de la concurrencia de ambos condicionantes: que el tratamiento de datos sea automatizado y que el responsable trate los datos con base en el consentimiento del interesado o en la necesidad de cumplir un contrato), y d) se introducía como limitación adicional (que luego pasara a ser una limitación más general) que inhibía el derecho a la portabilidad si la revelación de datos pudiera vulnerar derechos de propiedad intelectual.[108]

Así, con varios otros derechos[109] y nuevos principios,[110] los derechos al olvido y a la portabilidad encontraron eco normativo en el RGPD (artículos 13, 14, y 20 para el derecho a la portabilidad, y artículo 17 para el derecho al olvido) y en los proyectos de adecuación de las leyes nacionales europeas (v.gr., anteproyecto del Ministerio de Justicia español, que complementa brevemente al RGPD), pero no consiguieron similar reconocimiento en Iberoamérica.

En efecto, el derecho al olvido sólo obtuvo referencias implícitas en la regulación del derecho de oposición al tratamiento en la LGPDPPSO de México y en el proyecto de ley de protección de datos de Chile, ambas de 2017,[111] y no fue unánimemente acogido ni por las decisiones de los órganos de control ni por las resoluciones de los tribunales nacionales de clausura de

[108] Fernández, J. y Fernández, P. (2017). "El derecho a la portabilidad de los datos", en Piñar, J. (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. España: Reus, p. 257 y ss.

[109] Los de transparencia de la información (artículos 5, 12, 13, 14 y 88) y de limitación al tratamiento (artículos 18 y 19).

[110] Los de transparencia (5, 12, 13, 14, 26, 40, 41, 42, 43 y 88), responsabilidad o *accountablity* (artículos 24, 26 y 82) y protección de datos por defecto y desde el diseño (artículo 25).

[111] Artículo 47 de la ley mexicana y artículo 16, inc. b, del proyecto de ley de protección de datos chilena, que autorizan, respectivamente, a oponerse al tratamiento cuando "aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia cause un daño o perjuicio al titular" y cuando "el dato personal haya caducado".

la región. A la inversa, el derecho a la portabilidad —el único de los dos que mantuvo un buen grado de consenso—,[112] ganó expreso reconocimiento en 2017 en el artículo 57 de la LGPDPPSO de México y en el numeral 30 de los Estándares de protección de datos para los países Iberoamericanos aprobados por la Red Iberoamericana de Protección de Datos[113] y también, en el mismo año, fue incorporado en el proyecto de reforma a la ley de protección de datos personales de Argentina y en el proyecto de ley chilena de protección de datos personales.[114]

## II. Relevancia temática y contexto

La portabilidad, bien entendida, requiere que sean compatibles, no sólo los formatos de tratamiento, sino también de hardware y software. De hecho, la ejecutabilidad de un mismo software en diferentes plataformas es condición para un desafío mayor: el de la interoperabilidad de los sistemas, que al entenderse —en sus perspectivas técnica, organizativa y semántica— la habilidad de dos o más sistemas o componentes para intercambiar información y utilizarla intercambiada, se convierte es un concepto clave, tanto en el ámbito privado como en el público, con miras al gobierno electrónico, abierto y al desarrollo de los sistemas inteligentes.

Desde luego que la portabilidad exige la normalización de datos personales y no personales y debe alcanzar tanto al sector público como al privado, aunque actualmente no todas las regulaciones se refieren a ambos aspectos. En el ámbito de la Unión Europea existen diversas regulaciones que se ocupan de asegurar el libre flujo de ellos en el ámbito comunitario por medio de "políticas comunes respaldadas por redes y sistemas interconectados e interoperables"[115] y actualmente la Comisión Europea ha puesto a consideración un proyecto de reglamento destinado a asegurar el libre flujo de los datos no personales, el cual, como lo indica Peguera, complementa al RGPD, que está destinado a regular el tratamiento y libre flujo de los datos personales.[116]

[112] Pese a su reconocimiento jurisprudencial por el TJUE en el caso *Costeja*, este derecho se encuentra envuelto en fuertes polémicas e incluso de su primigenia inclusión, con cierto detalle, en el proyecto de Reglamento de 2012, apenas sobrevivió entre paréntesis y en el epígrafe del artículo referido al derecho de supresión (artículo 17), ubicación por lo demás también criticada por cuanto la eliminación de los datos no es el único medio de ejercer el derecho al olvido (v.gr., la Ley General de Protección de Datos mexicana y el proyecto de ley chilena de protección de datos de 2017 lo incorporan dentro del derecho de oposición al tratamiento).

[113] Adoptados en la XXV Cumbre Iberoamericana de Jefes de Estado y de Gobierno (Colombia, 28 y 29/10/16).

[114] Artículo 33 del proyecto de ley argentino y artículo 19 del proyecto chileno.

[115] Nuevo marco de interoperabilidad para los servicios públicos europeos 1 COM (2015) 192 final.

[116] Peguera, M. (2017). *Propuesta de Reglamento para facilitar la libre circulación de los datos no personales en la UE* [Mensaje en un blog]. CUATRECASAS. Disponible en: http://blog.cuatrecasas.com/propiedad-intelectual/propuesta-de-reglamento-para-facilitar-la-libre-circulacion-de-los-datos-no-personales-en-la-ue/, [fecha de consulta: 3 de mayo 2018].

## III. Análisis del contenido

El artículo 75 de la LGPDPPSO se inspiró en el artículo 18 del primer borrador del RGPD, de modo que existiendo abundante material de análisis respecto de la norma europea finalmente aprobada, nos ocuparemos primeramente de ésta, a fin de que tales elementos puedan ser utilizados como pautas interpretativas de los alcances de las disposiciones locales. Luego nos ocuparemos, con idéntico objetivo, de los Estándares Iberoamericanos aprobados por la RIPD (ya que México ha tenido un notable protagonismo en su confección) y finalmente, de la regla local.

### 1. El derecho a la portabilidad en el Reglamento Europeo de Protección de Datos

*Artículo 20*

*Derecho a la portabilidad de los datos*

1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:
   a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y
   b) el tratamiento se efectúe por medios automatizados.

2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.
3. El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.
4. El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.

Esta regla se complementa con otras referidas al ejercicio de los derechos del titular, como los artículos 12 (Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado); 13 (Información que deberá facilitarse cuando los datos personales se obtengan del interesado); 14 (Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado,

norma similar excepcionalmente aplicable), y 15 (Derecho de acceso del interesado, que señala la información que debe brindársele al interesado, incluyendo la disponibilidad de los otros derechos, pese a que no alude al derecho a la portabilidad, surge de su ubicación en el RGPD y de los artículos 13 y 14). A estos artículos deben adicionarse los considerandos 59,[117] 63 y 64,[118] 68,[119] 73[120] y 156[121] del Reglamento, que explican con detalle el sentido y alcance de las normas propuestas.

---

[117] Es obligación de los responsables del tratamiento: a) arbitrar fórmulas para facilitar al interesado el ejercicio de los derechos reconocidos en el Reglamento, incluidos los mecanismos para obtener gratuitamente "el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición" (se aprecia aquí también el mismo olvido que se detecta en el artículo 15, pues se omite referenciar al derecho a la portabilidad); b) proporcionar medios para que las solicitudes se presenten por medios electrónicos, en particular cuando los datos personales se tratan por esos medios, y c) responder a las solicitudes del interesado sin dilación indebida y a más tardar en el plazo de un mes, y explicar sus motivos en caso de que no fuera a atenderlas.

[118] Aludiendo al derecho de acceso se indica —en lo que al de portabilidad puede resultar aplicable—, que éste debe poder ser ejercido con facilidad (y, si es posible, a través del acceso remoto a un sistema seguro que ofrezca un acceso directo a los datos personales) por el interesado (para cuya identificación el responsable del tratamiento debe utilizar todas las medidas razonables, en particular en el contexto de los servicios en línea y los identificadores en línea), y que su ejercicio no debe afectar negativamente a los derechos y libertades de terceros (incluidos los secretos comerciales y la propiedad intelectual, particularmente sobre los programas informáticos), sin que ello resulte en la negativa del responsable del tratamiento a prestar toda la información o en la conservación de los datos personales con el único propósito de poder responder a eventuales solicitudes.

[119] Se indica aquí que con la inclusión del nuevo derecho se busca reforzar aún más el control sobre los propios datos, y que por ello se prevé que "cuando el tratamiento de los datos personales se efectúe por medios automatizados", los interesados que hubieran facilitado tales datos los deben recibir "en un formato estructurado, de uso común, de lectura mecánica e interoperable", a fin de poder transmitirlos a otro responsable, lo que obliga al responsable a "adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles", lo que lleva a alentar "a los responsables a crear formatos interoperables".

Y respecto de los límites al derecho, se advierte que "por su propia naturaleza" no resulta aplicable respecto de "responsables que traten datos personales en el ejercicio de sus funciones públicas" (cuando el tratamiento sea necesario para el ejercicio de poderes públicos o para cumplir una obligación legal o con una misión en interés público) y tampoco cuando el tratamiento no fuere necesario para la ejecución de un contrato con el titular o los datos no se hubiesen proporcionado a partir del consentimiento de éste. Se agrega finalmente que el ejercicio de este derecho no afecta el de otros derechos del interesado, como el de supresión de los datos personales (con sus límites), o el de mantener los datos que haya facilitado para la ejecución de un contrato (en la medida y durante el tiempo en que los datos sean necesarios para la ejecución de dicho contrato), y que tampoco debe afectar los derechos de otros interesados cuando un conjunto de datos personales determinado concierna a más de uno, hipótesis en la cual la satisfacción del derecho del solicitante debe modularse.

[120] Se afirma aquí que el Derecho de la Unión o de los Estados miembros puede imponer restricciones a determinados principios y a los derechos del interesado —entre los cuales menciona el derecho a la portabilidad— así como a determinadas obligaciones conexas de los responsables del tratamiento, pero ello sólo en la medida en que sea "necesario y proporcionado en una sociedad democrática" que se realice con determinados fines "interés público general de la Unión o de un Estado miembro" (menciona una importante cantidad de supuestos) o para la protección del interesado o de los derechos y libertades de otros "incluida la protección social, la salud pública y los fines humanitarios", y que dichas restricciones se ajusten "a lo dispuesto en la Carta y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales".

[121] Se trata aquí a las garantías adecuadas que deben rodear el tratamiento de datos con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, refiriendo en concreto a que los Estados miembros deben establecer garantías adecuadas y a que pueden establecer, bajo condiciones específicas y a reserva de garantías adecuadas para los interesados (tales como procedimientos concretos para el ejercicio de los derechos), especificaciones y excepciones con respecto a los requisitos de información y los derechos de rectificación, de supresión, al olvido, de limitación del tratamiento, a la portabilidad de los datos y de oposición.

El RGPD además prevé sanciones administrativas específicas que aplicará la autoridad de control competente para el supuesto en que no se satisfaga este derecho al cual pone en pie de igualdad a tales efectos con todos los contenidos entre los artículos 12 y 22.

**1.1. El derecho a la portabilidad en las "Directrices sobre el derecho a la portabilidad de los datos", del GT 29 (WP 29).** El Grupo de Trabajo del artículo 29 de la Directiva 95/46 (GT 29 o WP 29) aprobó, el 13 de diciembre de 2016, las Directrices sobre el derecho a la portabilidad de los datos (16/EN, GT242), donde se analizan los principales elementos constitutivos de este derecho, se establecen los supuestos de procedencia y se tratan otros aspectos particularmente relevantes que resultan de imprescindible consulta para establecer sus alcances por haber sido elaborado por el máximo órgano comunitario especializado en protección de datos.

**1.1.1. Naturaleza jurídica del derecho, objeto y finalidad.** El dictamen aclara, primeramente, que si bien este derecho está estrechamente relacionado con el de acceso, difiere de éste en muchos aspectos, siendo el propósito principal de su reconocimiento tanto el capacitar al interesado y darle más control sobre sus datos personales, como promover, a través de la transmisión directa de datos personales de un responsable a otro (lo que permite al titular de los datos cambiar entre diferentes proveedores), la libre circulación de datos personales en la UE, la competencia entre los responsables del tratamiento y el desarrollo de nuevos servicios en el contexto de la estrategia de mercado único digital.

Mencionan luego las Directrices del GT 29 que el RGPD "no establece un derecho general a la portabilidad de los datos", de manera que todos los datos personales estén alcanzados por este derecho, sino que sólo abarca a los que son objeto de tratamiento automatizado aportados con el consentimiento del interesado (6.1.a y 9.2.a); o por derivación de un contrato en el que éste sea parte (artículo 6.1.b), de manera que "cubre los datos proporcionados conscientemente y de forma activa por el interesado, así como los datos personales generados por su actividad".

Interpretando esta limitación, indica que la exigencia de que los datos sean proporcionados por el interesado incluye, tanto los entregados de manera consciente y activa (por ejemplo: datos de cuenta, que incluyen la dirección postal, el nombre de usuario y la edad presentados a través de formularios en línea) como los generados y recabados a partir de las actividades en respuesta a una solicitud de portabilidad de los datos (por ejemplo aquellos generados en bruto por un contador inteligente), categoría ésta que no incluye los generados exclusivamente por el responsable del tratamiento (como un perfil de usuario creado mediante el análisis de los datos en bruto de un contador inteligente),

que de todos modos quedan alcanzados por otros derechos del interesado, como a la información y de acceso.[122]

**1.1.2. Derechos del titular de los datos.** El RGPD, según se explica en el dictamen, le reconoce los siguientes derechos al titular de los datos que ejerce el derecho a la portabilidad:

**1.1.2.1. Derecho a recibir del responsable los datos personales requeridos, de manera gratuita, sin dilaciones indebidas y en un formato estandarizado que permita la interoperabilidad.** El artículo 12 RGPD estipula que toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 será gratuita para el titular de los datos, pero que cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá: a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información, comunicación o actuación solicitada o b) negarse a actuar respecto de la solicitud.

A tenor de estas propuestas, aclara el dictamen, si bien el responsable sólo podrá cobrar una tasa por facilitar los datos si se demostrara que las solicitudes son manifiestamente infundadas o excesivas, en lo que respecta a los servicios de la sociedad de la información u otros servicios en línea similares, especializados en el tratamiento de datos personales, es muy improbable que responder a múltiples solicitudes de portabilidad suponga en general una carga excesiva y además, el coste global de los procesos creados para responder a las solicitudes de portabilidad no debe tenerse en cuenta para determinar si es excesivo.

También se menciona que cuando para responder a la solicitud de portabilidad se deba recopilar un gran número de datos, que además se encuentren en una estructura compleja o presenten otros problemas técnicos, se abre un verdadero desafío para el responsable del tratamiento, porque debe proporcionar una visión general “de forma concisa, transparente, inteligible y fácilmente accesible, usando un lenguaje claro y sencillo” (artículo 12.1 RGPD) de tal modo que el interesado pueda usar aplicaciones informáticas para identificar, reconocer y procesar con facilidad datos específicos. Sugiere

[122] El dictamen indica que se incluyen entre los datos “proporcionados por el interesado” a los entregados en forma activa y consciente; a los datos “observados” en virtud del uso del servicio o el dispositivo (v.gr., el historial de búsqueda, los datos de tráfico y los datos de ubicación e incluso otros datos en bruto, como el ritmo cardiaco registrado por dispositivos de control de forma física y estado de salud), lo que implica que deben guardar relación con la actividad del interesado o derivarse de la observación de su comportamiento, pero no quedan incluidos los que se deriven del análisis posterior de dicho comportamiento, de modo que se excluyen los datos inferidos y los deducidos, creados por el responsable del tratamiento sobre la base de los proporcionados por el interesado (una puntuación crediticia o el resultado de un examen de salud de un usuario), ya que todos los datos personales generados por el responsable como parte del tratamiento de éstos (por ejemplo, mediante un proceso de personalización o recomendación, mediante categorización de usuarios o creación de perfiles), son datos que se deducen o se infieren de los aportados por el interesado.

el dictamen que, en tales casos, el responsable responda a las solicitudes ofreciendo una interfaz de programación de aplicación (por sus siglas, API) para que las personas puedan acceder a través de sus propios programas informáticos o con programas de terceros o bien autorizar a otros a hacerlo en su nombre (incluso a otro responsable).

En relación al plazo de respuesta, si bien el artículo 20 del RGPD no refiere —a diferencia de lo que ocurre con los otros derechos ARCO— a que se debe dar respuesta "sin dilación indebida", esto constituye un principio general contenido incluso en el considerando 59, que dispone al respecto que el responsable "debe estar obligado a responder a las solicitudes del interesado sin dilación indebida" (ya sea para admitirlas como para denegarlas), lo cual es relevante porque los responsables que operan servicios de la sociedad de la información son técnicamente capaces de cumplir con las solicitudes rápidamente y por ello, para satisfacer las expectativas de los usuarios, es recomendable definir previamente e informar a los interesados cuál será el plazo en el que puede darse respuesta al pedido.

El plazo máximo concedido al responsable —tanto para efectivizar como para denegar la solicitud— es general para el ejercicio de los derechos ARCO (artículos 12.3. y 12.4 RGPD), esto es el de "un mes a partir de la recepción de la solicitud", prorrogable por otros dos meses cuando sea "necesario, teniendo en cuenta la complejidad y el número de solicitudes", supuesto en el que debe informase al interesado antes del vencimiento del plazo general, e indicando los motivos de la dilación. Cuando la solicitud es denegada, se deberá informar al solicitante acerca de las razones de tal negativa y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar las acciones judiciales pertinentes.

En cuanto al formato en que se deberán entregar los datos, ante la amplia gama de datos que podría procesar un responsable, el RGPD no impone formato alguno, ya que el más apropiado diferirá entre los diversos sectores, pero exige que los que se escojan deben ser adecuados (lo que excluye a los sujetos a costosas limitaciones de licencia), contar con un elevado nivel de abstracción (en este aspecto, la portabilidad supone una capa adicional de tratamiento por parte de los responsables a fin de extraer los datos de la plataforma y excluir aquellos que sean portables, como las contraseñas de usuario, los datos de pago, los patrones biométricos, etc.) y permitir su reutilización. Así, al aludir a que deben entregarse "en un formato estructurado, de uso común y legible por máquina",[123] exige que el formato sea interoperable, término clave definido

[123] *Legible por máquina* es un término definido en el Considerando 21 de la Directiva 2013/37/UE (modificatoria de la Directiva 2003/98/CE relativa a la reutilización de la información del sector público) como un formato de archivos estructurado de forma que las aplicaciones informáticas

como “la capacidad de que organizaciones dispares y diversas actúen en pos de objetivos comunes mutuamente beneficiosos y acordados, en relación con la puesta en común de información y conocimiento entre las organizaciones, a través de los procesos empresariales que respaldan, mediante el intercambio de datos entre sus sistemas de TIC respectivos”.[124]

El considerando 68 aclara —y esto es relevante— que el derecho del interesado a transmitir o recibir datos personales “no debe crear la obligación para los responsables del tratamiento de adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles”, esto porque la portabilidad tiene por objetivo producir sistemas interoperables, no sistemas compatibles.

El GT 29 encomienda a las partes interesadas del sector y a las asociaciones comerciales a elaborar conjuntamente normas y formatos interoperables, reto abordado también por el Marco Europeo de Interoperabilidad (EIF, por sus siglas en inglés), que ha creado un marco consensuado de interoperabilidad para las organizaciones que presten conjuntamente servicios públicos, donde se abordan una serie de elementos comunes (vocabulario, conceptos, principios, políticas, directrices, recomendaciones, normas, especificaciones y prácticas).

**1.1.2.2. Derechos a obtener los datos personales para almacenarlos y a que se transmitan de un responsable del tratamiento a otro “sin impedimentos”.** El titular de los datos, al ejercer el derecho a la portabilidad, puede: a) obtener sus datos sólo para un uso personal posterior en un dispositivo privado, sin transmitirlos a otro responsable (como libros adquiridos *on line* o canciones escuchadas a través de un servicio específico), supuesto en el cual es claramente complementario el derecho de acceso (ya que ofrece una forma sencilla de gestionar y reutilizar los datos personales interoperables) y donde los responsables deben auxiliar a los usuarios a almacenar sus datos de modo no menos seguro que el del servicio en línea, recomendándole formatos y cifrados apropiados y b) solicitar la transmisión directa de sus datos a otro responsable, facultad que evita la retención de datos y a la vez promueve oportunidades de innovar al favorecer nuevos modelos de negocios, pues el intercambio compartido de datos entre organizaciones enriquece los servicios y las experiencias de los clientes, como ocurre en *Internet de las cosas* y en las *industrias del yo cuantificado*.

---

puedan fácilmente identificar, reconocer y extraer datos específicos, incluso exposiciones personales de hechos, y su estructura interna. Aclara luego que: a) los datos codificados en archivos que están estructurados en un formato legible por máquina son datos legibles por máquina; b) los formatos legibles por máquina pueden ser de uso libre o patentados; pueden ser estándares formales o no, y c) los documentos codificados en un formato de archivos que limita el tratamiento automático, debido a que sus datos no pueden extraerse o no pueden extraerse fácilmente, no deben considerarse que tienen un formato legible por máquina. Finalmente, la Directiva dispone que los Estados miembros deben alentar, cuando proceda, la utilización de formatos de uso libre y legibles por máquina.

[124] Artículo 2, Decisión nº 922/2009/CE relativa a las soluciones de interoperabilidad para las administraciones públicas europeas (ISA) OJ L 260, del 3 de octubre de 2009, p. 20.

**1.1.2.3. Derechos a cancelar los datos o a seguir usando los servicios del responsable del tratamiento aún después de haberse hecho efectivo el derecho a la portabilidad.** El ejercicio del derecho a la portabilidad, procure o no transmitir los datos a un tercero, no conlleva automáticamente el borrado de los datos de los sistemas del responsable, ya que no es condición para su ejercicio que el titular de los datos finalice la relación con aquél.

**1.1.2.4. Derecho a que no se extienda el período de retención bajo la excusa del ejercicio del derecho a la portabilidad.** El ejercicio del derecho a la portabilidad no resulta excusa válida para rechazar el pedido de cancelación de los datos que el responsable transmita, así como tampoco ese ejercicio puede afectar al período de retención original aplicable a los datos que se han transmitido. Además, la portabilidad de los datos no impone al responsable la obligación de retener los datos por más tiempo del necesario o más allá de un período de retención especificado; y no existe el requisito adicional de comenzar la retención simplemente para dar respuesta a una posible solicitud de portabilidad de datos.

**1.1.2.5. Derecho a ejercer el derecho de acceso emergente de la ley si un interesado descubre que los datos personales solicitados, de acuerdo con el derecho a la portabilidad de los datos, no responden plenamente a su solicitud.** Tanto de los principios generales del tratamiento de datos como de los derechos otorgados por la ley, es facultad del interesado ejercer el derecho de acceso a sus datos para poder verificar si la información se transfirió en el marco del ejercicio del derecho a la portabilidad.

**1.1.3. Deberes de los responsables del tratamiento (remitente y receptor).** En cuanto a las obligaciones que los responsables del tratamiento deben observar frente al ejercicio del derecho a la portabilidad, el dictamen enumera a los siguientes.

**1.1.3.1. Deber de informar a los interesados acerca de la disponibilidad del nuevo derecho a la portabilidad.** Con base en los artículos 13.2.b y 14.2.c, el titular de los datos cuenta con el derecho a ser informado por el responsable sobre la posibilidad de ejercer el derecho a la portabilidad, en especial con antelación al cierre de cualquier cuenta, debiendo asegurarse de distinguirlo claramente de los otros derechos y de indicar qué tipos de datos puede recibir usando el derecho de portabilidad o el derecho de acceso.

**1.1.3.2. Deber de transmitir los datos con seguridad y a la persona adecuada.** Dado que el ejercicio de este derecho puede plantear problemas de seguridad (como transmitir datos personales desde un sistema de información), el responsable del tratamiento debe garantizar “la seguridad adecuada de los datos personales, incluyendo la protección contra tratamientos no autorizados

o ilícitos y contra su pérdida accidental, destrucción o daños, utilizando medios técnicos y organizativos apropiados", y por derivación del deber general del artículo 5.1.f del RGPD (integridad y confidencialidad), se deben tomar todas las medidas de seguridad requeridas para garantizar que los datos personales se transmitan de forma segura (por ejemplo, mediante el uso de cifrado) al destinatario correcto (mediante el uso de información de autentificación adicional), pero éstas no deben obstruir el ejercicio de los derechos de los usuarios (imponiendo costes adicionales).

**1.1.3.3. Deber de autenticar debidamente al solicitante.** El responsable debe identificar debidamente a quien ejerce cualquiera de los derechos previstos por la norma, pero tal deber debe flexibilizarse de acuerdo con los artículos 11.2, 12.2 y 12.6 del RGPD, distinguiéndose los casos de innecesariedad de identificación, imposibilidad de identificación y duda razonable de identidad, donde se requiere la aportación de información adicional. Además, cuando la información y los datos recabados en línea estén vinculados a seudónimos o identificadores exclusivos, los responsables pueden implementar procedimientos apropiados de autenticación (como nombres de usuario y contraseñas para acceder a cuentas de correo electrónico, redes sociales y cuentas utilizadas para otros diversos servicios en los cuales los usuarios prefirieron no revelar su nombre e identidad completos).

**1.1.3.4. Deber de limitarse a proveer datos personales que incumban al interesado.** El ejercicio del derecho no autoriza a transferir datos personales no referidos al interesado, incluso los anónimos, salvo que se trate de "datos seudónimos que estén claramente vinculados con el interesado, (p.ej. al haber éste proporcionado el identificador correspondiente, cfr. artículo 1, apartado 2)" o que no hayan sido proporcionados por éste.

El dictamen pone en claro que cuando la información contenga datos personales referidos a varios interesados que no han dado su consentimiento, los responsables del tratamiento "no deberán tener una interpretación excesivamente restrictiva" de la norma, porque, por ejemplo, los registros telefónicos pueden incluir en el historial de la cuenta del abonado detalles de terceros participantes en llamadas entrantes y salientes y aunque los registros contengan datos personales referentes a multitud de personas, no puede negarse la portabilidad, sino que sólo implicará que si tales registros se transmiten a un nuevo responsable del tratamiento, éste no debe procesarlos para ningún fin que pueda afectar negativamente los derechos y libertades de los terceros.

Del mismo modo amplio debe considerarse al concepto de *datos que haya facilitado* el interesado, incluyéndose a todos los datos observados acerca del interesado durante las actividades para cuyo fin se los han recabado (como

puede ser un historial de transacciones o un registro de accesos) y también a los datos recabados mediante el seguimiento y registro del interesado, se transmitan o no de manera activa o consciente (por ejemplo, una aplicación que registre el ritmo cardíaco o los hábitos de navegación).[125]

**1.1.3.5. Deber de limitarse a proveer datos personales que no afecten negativamente a los derechos y libertades de terceros.** Se configura la hipótesis de afección negativa a los derechos y libertades de terceros, por ejemplo, en la hipótesis contemplada en el considerando 63 del RGPD de "los secretos comerciales o la propiedad intelectual y en particular los derechos de autor que protegen los programas informáticos" y cuando la transmisión impide a terceros ejercer sus derechos a la información, al acceso, etc. Por ello, cuando en el conjunto de datos se incluyan datos personales de terceros, debe señalarse otro motivo de la legalidad del tratamiento como un interés legítimo del responsable receptor de los datos, según el artículo 6.1.f, o cuando el propósito del responsable del tratamiento es proporcionar un servicio al interesado que permita a éste procesar datos personales para una actividad puramente personal o doméstica, como por ejemplo cuando se pretende portar los correos electrónicos y las cuentas bancarias que contienen datos de terceros que interactúan con el titular.

Con el objeto de reducir aún más los riesgos para otros interesados cuyos datos personales pueden ser transferidos, el dictamen alienta a todos los responsables del tratamiento (remitentes y receptores) a que pongan en práctica herramientas que permitan a los interesados seleccionar los datos relevantes y excluir, donde proceda, otros datos suyos, así como mecanismos de autorización para otros interesados involucrados a fin de facilitar la transmisión de datos en aquellos casos en los que las partes estén dispuestas a dar su consentimiento porque también deseen trasladar sus datos a algún otro responsable del tratamiento, situación que podría darse en las redes sociales.

**1.1.3.6. Deber de omitir retener los datos personales.** El responsable no debe retener los datos más tiempo del necesario o del período de retención especificado, y debe evitar retenerlos simplemente para dar respuesta a una posible solicitud de portabilidad de datos.

[125] Se aclara en el dictamen que resulta improbable que los derechos y libertades de los terceros se vean afectados negativamente en la transmisión por correo electrónico o del historial bancario, si sus datos se utilizan para el mismo propósito en cada tratamiento (es decir, como dirección de contacto usada sólo por el interesado o como historial de una de las cuentas del interesado), y a la inversa, sus derechos y libertades no se respetarán si el nuevo responsable del tratamiento usa el listado de contactos con fines de marketing, de modo que, a fin de evitar efectos negativos sobre los terceros involucrados, el tratamiento de dicho listado por parte de otro responsable del tratamiento se permite sólo en la medida en que los datos se mantengan bajo el control exclusivo del usuario solicitante y se gestionen por necesidades puramente personales o domésticas.

En el caso del receptor de los datos, debido a que se convierte en nuevo responsable del tratamiento, también debe omitir la retención de datos irrelevantes para el servicio que se prestará (v.gr., si se solicita la transmisión de las transacciones bancarias a un servicio que ayude a la gestión de su presupuesto, el nuevo responsable del tratamiento no necesita retener todos los datos de las transacciones una vez que han sido etiquetadas).

**1.1.3.7. Deber de ofrecer diferentes opciones de puesta en práctica del derecho.** El derecho a la portabilidad debe ser satisfecho bajo diferentes modalidades de acuerdo con la conveniencia del titular de los datos, como la descarga directa o la transmisión directa a otro responsable a través de una interfaz de programación de aplicación (API)[126] y por ello se recomienda desarrollar procedimientos para responder de forma automática a las solicitudes de portabilidad, por ejemplo, la descarga sencilla de archivos del impuesto sobre la renta prestada por un servicio gubernamental.

**1.1.3.8. Deber de los receptores de los datos portados de informar sobre la naturaleza de los datos personales que sean relevantes para la ejecución de sus servicios y de garantizar que tales datos sean pertinentes y no excesivos en relación con el nuevo tratamiento de datos.** Dado que todo nuevo tratamiento de los datos debe ajustarse a los principios y a las exigencias del RGPD, los receptores de los datos deben: a) proporcionar a los interesados información completa sobre la naturaleza de los datos personales relevantes para la ejecución de sus servicios, dado que con tal práctica se permite a los usuarios limitar los riesgos para terceros y también cualquier otra duplicación innecesaria de datos personales incluso cuando no haya otros interesados involucrados y b) informar sobre la naturaleza de los datos personales que sean relevantes para la ejecución de sus servicios, en el caso de una solicitud hecha a un servicio de *webmail* para recuperar correos electrónicos con la finalidad de enviarlos a una plataforma de almacenamiento segura, el nuevo responsable no necesita procesar los datos de contacto de los destinatarios, pues tal información no es relevante en relación con el propósito del nuevo tratamiento.

## 2. La portabilidad en los estándares de protección de datos para los países Iberoamericanos.

Con antecedente mediato en las Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana,[127] partiendo de las novedades aportadas por el RGPD y considerándolo un “marco normativo que

[126] Una API es un conjunto de definiciones, protocolos y herramientas de subrutinas para desarrollar programas y aplicaciones, y que traducido a términos más generales consistiría en “interfaces de aplicaciones o servicios web que ponen a disposición los responsables del tratamiento para que otros sistemas o aplicaciones pueden enlazarse y trabajar con sus sistemas”.

[127] Documento aprobado por la Red Iberoamericana de Protección de Datos en 2006 en Santa Cruz de la Sierra, con el objeto de contribuir a la elaboración de las iniciativas regulatorias de la protección de datos que surjan en la Comunidad Iberoamericana.

se posiciona como un referente obligado y determinante para la elaboración de las legislaciones nacionales de protección de datos en Iberoamérica", la RIPD aprobó en junio de 2017 los Estándares de protección de datos para los países Iberoamericanos, donde además de otras normas que resultan aplicables de manera específica tanto a los derechos ARCO como al derecho a la portabilidad y de un considerando explica el sentido de este derecho. El estándar 30, dividido en cuatro parágrafos, regula este derecho en sintonía con las reglas emergentes del RGPD para los casos en que los datos se traten por vía electrónica o medios automatizados.

Estos estándares ofrecen una versión sintética tanto de los considerandos como del articulado del RGPD y de las directrices sobre el derecho a la portabilidad de dato aprobadas por el GT 29, de manera que, aun dejando espacio para mayor detalle en las legislaciones nacionales (por ejemplo, para su extensión respecto de todo tipo de responsables de tratamiento), constituyen un punto de partida técnicamente sólido para la homogeneización de las normas locales en el ámbito latinoamericano.

Entre sus principales normas se advierte sobre la necesidad de adoptar un marco regulatorio que garantice el derecho a la protección de datos a partir del ejercicio gratuito de los derechos en él reconocidos, incluso respecto de motores de búsqueda de internet (considerando 19).

Por su parte, el estándar 16, al regular el principio de transparencia, carga al responsable el deber de informar al titular de los datos sobre la existencia y características del tratamiento, incluyendo la "existencia, forma y mecanismos o procedimientos a través de los cuales podrá ejercer los derechos de acceso, rectificación, cancelación, oposición y portabilidad".

En cuanto al ejercicio de los derechos ARCO y a la portabilidad se expresa que "en todo momento" se puede solicitar el acceso, rectificación, cancelación, oposición y portabilidad de los datos personales, y que el ejercicio de cualquiera de éstos no es requisito previo, ni impide el ejercicio de otro (estándar 24), y que el responsable debe establecer medios y procedimientos sencillos, expeditos, accesibles y gratuitos para el ejercicio de tales derechos, y que la ley debe establecer los requerimientos, plazos, términos y condiciones en que los titulares podrán ejercerlos, así como las causales de improcedencia, respecto de las cuales realiza una enunciación no taxativa (estándar 32).

Además de estas referencias, el estándar 30 del documento establece específicamente:

> 30 (Derecho a la portabilidad de los datos personales)
>
> 30.1. Cuando se traten datos personales por vía electrónica o medios automatizados, el titular tendrá derecho a obtener una copia de los datos personales que hubiere proporcionado al responsable o que sean objeto de tratamiento, en un formato electrónico estructurado, de uso común y lectura mecánica, que le permita seguir utilizándolos y transferirlos a otro responsable, en caso de que lo requiera.
>
> 30.2. El titular podrá solicitar que sus datos personales se transfieran directamente de responsable a responsable cuando sea técnicamente posible.
>
> 30.3. El derecho a la portabilidad de los datos personales no afectará negativamente a los derechos y libertades de otros.
>
> 30.4. Sin perjuicio de otros derechos del titular, el derecho a la portabilidad de los datos personales no resultará procedente cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles.

## 3. La portabilidad en la LGPDPPSO.

Esta norma, aprobada en 2017, tomó como principal fuente, como ya fue señalado, a la primera propuesta de RGPD de 2012 y reprodujo casi literalmente el artículo 18 en este artículo 57, que también está compuesto por tres párrafos y se encuentra en el último de los tres capítulos que regulan los derechos del titular de los datos.

Así, en el Título Tercero (Derechos de los titulares y su ejercicio) integrado por los artículos 43 a 57 y luego de los dos capítulos destinados a los derechos ARCO y su ejercicio, la regla trata el derecho a la portabilidad en el único artículo que integra el último capítulo, con una técnica legislativa que, en este punto, se aparta de la del RGPD finalmente aprobado, que los trata de manera conjunta, más allá de que los reconozca en artículos diferentes.

La única regla que se refiere a este derecho es, por un lado, más breve y más abierta que la del RGPD (podría de todos modos interpretarse conceptualmente más limitada en cuanto requiere que los datos personales se traten por vía electrónica y parece no incluir a todos los que estén

automatizados, pero hoy la diferencia es casi meramente semántica) porque no exige que los datos hayan sido obtenidos directamente del titular o provengan de un contrato.

Por otro lado, no tiene el mismo alcance que el RGPD desde que esta ley se refiere exclusivamente al tratamiento de datos en posesión de los sujetos obligados y no a los que se encuentran en posesión de particulares, que están regidos por la LFPDPPP aprobada en 2010, la cual destina los capítulos III y IV a regular los derechos ARCO y su ejercicio de manera simétrica con la estructura y principios generales que luego se incorporarían en la LGPDPPSO y que no se refiere en modo alguno al derecho a la portabilidad.

La LGPDPPSO, al igual que su par europea, prevé ser complementada por el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (así como la Comisión Europea lo hace para el RGPD) a través de lineamientos en los cuales se fijan los parámetros a considerar para determinar los supuestos en los que se está en presencia de un formato estructurado y comúnmente utilizado, así como las normas técnicas, modalidades y procedimientos para la transferencia de datos personales.

La ley omite otras referencias a la portabilidad, de modo que, para que opere eficazmente, debe considerársela, como ocurre en el RGPD, un derecho ARCO más y aplicarle, en todo lo que no resulten incompatibles, los principios generales y las reglas previstas para el ejercicio de los derechos ARCO (artículos 43 a 56). Al respecto cabe destacar que el titular:

a) “En todo momento” podrá solicitar al responsable la portabilidad respecto de los datos que le conciernan, sin que el ejercicio de cualquiera de los derechos ARCO sea requisito previo, ni impida su ejercicio (artículo 43).
b) Podrá “conocer la información relacionada con las condiciones y generalidades de su tratamiento” (artículo 44).
c) Se sujetará al procedimiento establecido en la ley y demás disposiciones que resulten aplicables en la materia respecto de la recepción y trámite de las solicitudes para el ejercicio de este derecho que se formulen a los responsables (artículo 48).
d) Deberá acreditar su identidad para su ejercicio o en su caso, “la identidad y personalidad con la que actúe el representante”, salvo algunas excepciones puntuales (artículo 49).
e) Ejercerá su derecho gratuitamente y sólo se le cobrarán los costos de reproducción, certificación o envío conforme a la normatividad aplicable no pudiendo establecer para la presentación de las solicitudes servicios o medios que impliquen un costo al titular (artículo 50).
f) Deberá poder contar con procedimientos sencillos que permitan el ejercicio de su derecho.

g) Obtendrá respuesta en un plazo no mayor a 20 días a partir del día siguiente a la recepción de la solicitud o 20 cuando así lo justifiquen las circunstancias, y siempre y cuando se le notifique dentro del plazo de respuesta, debiéndose satisfacer el derecho en no más de 15 días desde el día siguiente en que se haya notificado la respuesta al titular (artículo 51).

h) Sólo cumplimentará los requisitos para solicitar el ejercicio de los derechos ARCO y los que sean obviamente inherentes al pedido de portabilidad que se desprende del artículo 57 y con el trámite y efectos previstos en la ley (artículos 52 y 53).

i) Sólo podrá ver rechazado su pedido por las causales contenidas en la ley (artículo 55).[128]

j) Deberá ser informado del motivo de la determinación con fundamento en los motivos previstos en el artículo 55 en el plazo de hasta 20 días y por el mismo medio en que se llevó a cabo la solicitud, pudiendo interponer el recurso de revisión previsto en el artículo 94 de la misma ley contra la negativa de dar trámite a su solicitud y también frente a la falta de respuesta (artículos 55 y 56).

k) Podrá denunciar la transgresión de sus derechos (incluido el de portabilidad, que no se encuentra expresamente mencionado) a fin de que se evalúe la aplicación de sanciones cuando se vulneren principios básicos del tratamiento (artículo 163).

3.1. Los Lineamientos que establecen los parámetros, modalidades y procedimientos para la portabilidad de datos personales. El pleno del INAI aprobó, en sesión del 6 de noviembre de 2017, un anteproyecto de Lineamientos que fueron remitidos al Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales en función de lo dispuesto por el artículo 57 y quinto transitorio de la LGPDPPSO. Realizada su revisión, fueron aprobados mediante la resolución CONAIP/SNT/ACUERDO/EXT01-23/01/2018-03 y publicados en el DOF el 12 de febrero de 2018.

El documento consta de 27 artículos, desplegados en cuatro capítulos. El primero de ellos (De las disposiciones generales) indica que los lineamientos tienen por objeto establecer los parámetros para determinar los supuestos

[128] En concreto, las causales de falta de acreditación de identidad, inexistencia de datos en posesión del responsable, impedimento legal, lesión a los derechos de un tercero, obstaculización de actuaciones judiciales o administrativas, resolución de autoridad competente que restrinja el acceso a los datos o vede la portabilidad, cuando la transferencia de los datos haya sido previamente realizada, cuando el responsable no sea competente, cuando los datos sean necesarios para proteger intereses jurídicamente tutelados del titular o para dar cumplimiento a obligaciones legalmente adquiridas por él, cuando en función de sus atribuciones legales el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado mexicano, o cuando los datos personales sean parte de la información que las entidades sujetas a la regulación y supervisión financiera del sujeto obligado hayan proporcionado a éste, en cumplimiento a requerimientos de dicha información sobre sus operaciones, organización y actividades.

en los que se está en presencia de un formato estructurado y comúnmente utilizado, así como las normas técnicas, modalidades y procedimientos para la transmisión de datos personales, y luego de formular las necesarias definiciones de los términos técnicos utilizados se refiere a los ámbitos de validez subjetivo, objetivo y territorial (artículos 1 a 5).

En el segundo (Del objeto y alcance de la portabilidad de los datos personales), establece, primeramente, que se está ante un formato estructurado y comúnmente utilizado cuando: a) se trate de un formato electrónico accesible y legible por medios automatizados, de tal forma que éstos puedan identificar, reconocer, extraer, explotar o realizar cualquier otra operación con datos personales específicos; b) el formato permita la reutilización y/o aprovechamiento de los datos personales y c) el formato sea interoperable con otros sistemas informáticos (artículo 6).

Luego, indica que el objeto central de la portabilidad consiste en que el titular de los datos obtenga: a) una copia de los datos personales que facilitó directamente al responsable, en un formato interoperable que le permita usarlos y en su caso transmitirlos, y b) la transmisión de sus datos personales a un responsable receptor, siempre y cuando sea técnicamente posible, el titular hubiere facilitado directamente sus datos al responsable transmisor y el tratamiento se base en su consentimiento o en un contrato (artículo 7).

A continuación, expresa que la portabilidad sólo procede cuando: a) el tratamiento se efectúe por medios automatizados o electrónicos y en un formato estructurado y comúnmente utilizado; b) tales datos se encuentren en posesión del responsable o sus encargados; c) los datos conciernan al titular o a una persona física fallecida vinculada al interesado; d) el titular haya proporcionado directamente al responsable sus datos personales de forma activa y consciente (concepto que incluye los datos personales obtenidos en el contexto del uso, la prestación de un servicio o realización de un trámite, o bien aquellos proporcionados por el titular a través de un dispositivo tecnológico) y e) la portabilidad no afecte los derechos y libertades de terceros. Agrega que la portabilidad también procederá cuando exista una relación jurídica entre el responsable receptor y el titular, se dé cumplimiento a una disposición legal o el titular pretenda ejercer algún derecho (artículo 8).

También indica que el ejercicio del derecho impone la obligación al responsable de procesar, filtrar, seleccionar, extraer y diferenciar los datos que son objeto de portabilidad respecto a otra información que no lo sea, en concreto aquella: a) inferida, derivada, creada, generada u obtenida a partir del análisis o el tratamiento efectuado por el responsable sobre los datos proporcionados directamente por el titular como los datos sometidos a un proceso de personalización, recomendación, categorización o creación

de perfiles; b) presentada bajo seudónimos, salvo que éstos se encuentren claramente vinculados al titular y puedan identificarlo o lo hagan identificable cuando el responsable cuente con información adicional que permita su identificación o c) disociada, de tal manera que no puedan asociarse al titular ni permitir su identificación, salvo por un procedimiento posterior (artículo 9).

Se aclara a continuación que la portabilidad de los datos personales no impone obligación alguna al responsable de almacenar, preservar, guardar, mantener o conservar todos los datos en un formato estructurado y comúnmente utilizado, sólo para garantizarla (artículo 10).

Acerca de los deberes de información se indica que, mediante el aviso de privacidad se deberá señalar al titular de los datos la posibilidad de solicitar la portabilidad de sus datos personales y su alcance; los tipos o categorías de datos personales que técnicamente sean portables; el o los tipos de formatos estructurados y comúnmente utilizados disponibles para obtener o transmitir sus datos personales, así como los mecanismos, medios y procedimientos disponibles para que el titular pueda solicitar la portabilidad (artículo 11).

Con respecto a los efectos del ejercicio del derecho, indica que una petición de portabilidad no implica el cese o la conclusión de la relación jurídica con el responsable, por lo que el titular podrá seguir utilizando o beneficiándose del servicio o programa proporcionado por el responsable al que hubiere facilitado los datos personales (artículo 12).

Finalmente, se establece que los datos portables deben ser tratados de acuerdo con todos los principios, deberes y demás obligaciones que rigen el tratamiento de datos personales establecidos en la ley general o las leyes estatales en la materia (artículo 13).

En el capítulo III (De las reglas específicas para el ejercicio de la portabilidad de datos personales), se estipula, primeramente, que para el ejercicio de la portabilidad de datos personales el responsable debe observar, además de lo dispuesto en este capítulo, los requisitos, plazos, términos, condiciones y procedimientos establecidos en el Capítulo II del Título III de la ley general o en su caso de las leyes estatales en la materia (artículo 14).

Luego se indica que en la solicitud de portabilidad, sin perjuicio de lo dispuesto en el artículo 52 de la ley general, no pueden imponerse mayores requisitos que los de: a) la petición de copia o transmisión; b) la explicación acerca de la existencia de una situación de emergencia del titular a fin de la reducción de los plazos de respuesta, y c) la denominación del responsable receptor y el documento que acredite la relación jurídica entre el responsable y el titular o la existencia de una disposición legal habilitante o derecho que se pretende ejercer,

si se solicita la transmisión de los datos. La regla agrega que si el titular solicita copia puede acompañar el medio de almacenamiento o de lo contrario será provisto por el responsable cobrándole un costo razonable (artículo 15) de modo que la gratuidad emergente del artículo 50 de la ley general y de las legislaciones estatales no alcanza a la provisión del medio de almacenamiento (artículo 16).

También se establece que el responsable deberá: a) en el análisis de la procedencia de la solicitud, privilegiar la interpretación más amplia sobre los datos personales que conciernen al titular, con la salvedad de los supuestos de información inferida o de la presentada bajo seudónimos o disociada que no hagan identificable al titular (artículo 17); b) transmitir, en la medida de lo posible, el mayor número de metadatos que se hubieren generado y obtenido a partir del tratamiento de los datos personales proporcionados directamente por el titular (artículo 18); c) acortar en situaciones de emergencia el plazo de respuesta a diez días y el de efectivización de portabilidad a siete (artículos 19 y 21) y d) una vez que declaró procedente la solicitud, debe otorgar un plazo de tres días para a que el titular acompañe el medio de almacenamiento e informar, al mismo tiempo, del costo del medio si el titular decidiera no proporcionarlo, otorgándole no menos de tres días para su pago, en ambos casos debe señalar la existencia de la vía recursiva de revisión ante el INAI u otros organismos garantes estatales (artículo 20).

La norma dispone que el responsable podrá negar la portabilidad cuando se trate de información inferida, seudonimizada o disociada (artículo 23) y que la portabilidad se haga efectiva cuando el titular reciba una copia de sus datos en un formato estructurado y comúnmente utilizado que le permita seguir usándolos o hubiere sido notificado que el responsable transmisor, ante el cual ejerció la portabilidad de sus datos personales, transmitió éstos al responsable receptor conforme a sus instrucciones, agregando que si el titular no recogiera el medio de almacenamiento, la Unidad de Transparencia del responsable deberá tener a disposición una copia durante un plazo máximo de 60 días, transcurridos los cuales procederá al borrado seguro de los datos, sin que esto afecte a un nuevo ejercicio del derecho (artículo 22).

A continuación se deja en claro que el titular, su representante o quien acredite tener interés jurídico o legítimo respecto de datos personales de fallecidos podrán interponer recurso de revisión ante el INAI o ante los organismos garantes contra la respuesta o falta de ésta (artículo 24).

En el Capítulo IV (De las normas técnicas y procedimientos para la transmisión de datos Personales) indica, primeramente, que el responsable deberá considerar, al menos, una serie de normas técnicas que (artículo 25[129])

[129] Como mínimo: I) implementar mecanismos, medios y procedimientos idóneos que permitan al titular obtener sus datos personales, sea de manera personal, por vía electrónica, a través de opciones de descarga establecidas en sus páginas oficiales de internet, o por cualquier otra tecnología que considere pertinente; II) informar al titular sobre el o los tipos de formatos estructurados y comúnmente utilizados disponibles, a través de los cuales podrá entregar o transmitir los datos

establece las condiciones técnicas que deben observarse, tanto con carácter previo a la transmisión de los datos personales, (artículo 26[130]) como para la transmisión en sí misma de éstos (artículo 27[131]).

Finalmente, en los tres transitorios que coronan la regla, se establece que los lineamientos entrarán en vigor a los 180 días de su publicación en el DOF;

---

personales al responsable receptor, en función de la naturaleza de los datos personales y la viabilidad para ser objeto de portabilidad, y cuando sea técnicamente posible, otorgar al titular la elección del formato de entrega o transmisión de los datos; III) garantizar, en lo posible, la interoperabilidad del formato estructurado y comúnmente utilizado en el que se entreguen los datos a fin de su reutilización uniforme y eficiente y IV) procurar que los servicios y sistemas electrónicos en su posesión mantengan la capacidad de interoperar con otros sistemas como una cualidad integral desde su diseño y a lo largo de su ciclo de vida, adoptando protocolos y estándares que permitan el intercambio de datos personales entre diversos sistemas o plataformas tecnológicas, con independencia del lenguaje de programación o plataforma en la que fueron desarrollados.

130 En concreto, el responsable transmisor y el responsable receptor deben adoptar: I) protocolos, herramientas, aplicaciones o servicios que permitan el enlace y comunicación eficiente de los datos personales en un formato estructurado y comúnmente utilizado; II) medidas de seguridad de carácter administrativo, físico y técnico para la transmisión de los datos personales en un formato estructurado y comúnmente utilizado como son, de manera enunciativa mas no limitativa, mecanismos de autenticación de usuarios, conexiones seguras, o bien, utilizar medios electrónicos de transmisión cifrados; III) mecanismos de autenticación para el envío y recepción de los datos personales en un formato estructurado y comúnmente utilizado, los cuales deberán ser de uso exclusivo de éstas, y IV) controles que les permitan obtener evidencia sobre el envío, recepción e integridad de los datos personales transmitidos, en un formato estructurado y comúnmente utilizado. Agrega la norma que: V) Los sistemas o plataformas electrónicas utilizadas para el envío y recepción de los datos personales en un formato estructurado y comúnmente utilizado, deberán llevar un registro de todas las acciones u operaciones realizadas con las transmisiones de éstos como son, de manera enunciativa mas no limitativa, la persona que está autorizada para transmitir los datos personales; la fecha y hora en que se efectuó la transmisión; la fecha y hora en que se recibieron los datos personales en el sistema o plataforma electrónica; la persona autorizada para recibir los datos personales; si la transmisión fue exitosa o fallida y cualquier otra información que se genere con la misma.

131 La norma indica el siguiente procedimiento para la transmisión: I) La Unidad de Transparencia del responsable transmisor deberá dar respuesta al titular sobre la procedencia jurídica y técnica de la transmisión de sus datos personales en el plazo previsto en el artículo 51, párrafo primero de la Ley General o los que corresponda en las legislaciones estatales en la materia, salvo que el titular se encuentre en una situación de emergencia; II) El responsable transmisor deberá transmitir los datos personales, en un formato estructurado y comúnmente utilizado, al responsable receptor dentro del plazo a que se refiere el artículo 51, último párrafo de la Ley General o los que correspondan en las legislaciones estatales en la materia, salvo que el titular se encuentre en una situación de emergencia; III) El responsable transmisor deberá enviar los datos personales, en un formato estructurado y comúnmente utilizado, al responsable receptor, previa acreditación de la identidad del titular y, en su caso, la identidad y personalidad de su representante; IV) El responsable transmisor deberá cifrar los datos personales, en un formato estructurado y comúnmente utilizado, durante su envío al sistema o plataforma electrónica del responsable receptor; V) El responsable transmisor y el responsable receptor deberán autorizar a una persona que se encargue de vigilar que en la transmisión de los datos personales se observen las condiciones, normas, procedimientos y obligaciones técnicas previstas en los presentes Lineamientos en todo aquello que resulte aplicable; VI) La Unidad de Transparencia del responsable transmisor y la Unidad de Transparencia del responsable receptor coadyuvarán, en el ámbito de sus respectivas competencias, con la persona a que se refiere la fracción anterior del presente artículo para vigilar el cumplimiento de los presentes Lineamientos en la transmisión de los datos personales; VII) La Unidad de Transparencia del responsable receptor deberá notificar a la Unidad de Transparencia del responsable transmisor y al titular la recepción de los datos personales, en un formato estructurado y comúnmente utilizado, a más tardar al día siguiente de la recepción de éstos, y VIII) Las Unidades de Transparencia del responsable transmisor y del responsable receptor deberán coordinar la atención de las solicitudes de portabilidad de datos personales, sin que ello implique realizar o intervenir en el desarrollo de actividades de índole técnico propias de las unidades administrativas competentes.

que las Comisiones de Protección de Datos Personales y de Tecnologías de la Información y Plataforma Nacional de Transparencia del Sistema Nacional de Transparencia deberán elaborar una ruta crítica para el cumplimiento de los presentes lineamientos respecto de las implicaciones que tendría su entrada en vigor (a partir de los procesos, flujos, plazos y formatos que establezcan ambas comisiones unidas) y que el Sistema Nacional de Transparencia podrá constituir grupos de trabajo interdisciplinarios que tengan por objeto analizar, definir y proponer la adopción de estructuras mínimas de datos personales y estándares mínimos de seguridad y de comunicación e interoperabilidad de sistemas aplicables a sectores específicos, así como mejores prácticas que coadyuven al cumplimiento de estos lineamientos.

## IV. Conclusiones

El derecho a la portabilidad es un derecho sumamente técnico pero también trascendental, como lo es el objetivo final del logro de una interoperabilidad de los sistemas que coadyuva sin duda alguna a superar diversas trabas que derivan tanto de la acción o inacción de los gobiernos como de estrategias desplegadas en el sector privado que tienden al mantenimiento de "clientelas cautivas" de sus sistemas (*vendor lock-in*).

Más allá de las dificultades prácticas que conlleva el ejercicio del derecho, "su necesidad no debería ser objeto de discusión, dado el actual contexto digital, en el que ingente cantidad de información personal textual y multimedia se mueve por las diferentes redes sociales, o por los servicios de *cloud computing*, donde a unos y otros se les confía el almacenamiento y procesamiento masivo de información personal, lo que obliga a prever mecanismos que eviten, aduciendo cuestiones tecnológicas, el 'secuestro' de la información o el acabar como 'cautivos digitales' de por vida de un proveedor concreto. Intuitivamente el derecho a la portabilidad de los datos parece aportar mecanismos efectivos de protección frente al desarrollo de servicios y modelos de negocio que se han generado en torno a la red".[132]

Es cierto que "resulta difícil imaginar hasta qué punto el cliente de un servicio de banca en línea podrá ejercer su derecho a transmitir su información a otra entidad financiera, o por ejemplo, lo interesante que sería que un vendedor de productos en línea pudiera transferir la información de su perfil de ventas (en definitiva su prestigio digital como vendedor) a otra plataforma de subastas, y no tener que empezar desde cero a generar confianza en los compradores de la nueva plataforma a la que se ha trasladado",[133] pero los esfuerzos por instalar con el mayor alcance posible este nuevo derecho siempre serán bienvenidos.

---

[132] Miralles, R. (2012). *El derecho de la portabilidad de los datos personales*. Disponible en: http://www.abogacia.es/2012/11/15/el-derecho-de-la-portabilidad-de-los-datos-personales/.

[133] *Idem*.

Por su complejidad técnica queda un largo camino reglamentario por recorrer tanto para la Comisión Europea, en el ámbito de la Unión, como en el del Sistema Nacional de Transparencia para el caso de México, pero sus experiencias constituirán un valiosísimo aporte para los países iberoamericanos que ya han "puesto proa" hacia el reconocimiento de este derecho y hacia allí habrá que dirigirse, haciendo camino al andar.

## Referencias

Criado, I. *et al.* (2010). *Bases para una Estrategia Iberoamericana de Interoperabilidad*. [Archivo PDF]. Disponible en: http://siare.clad.org/siare/innotend/gobelec/BasesEstrategiaIberoamericanaInteroperabilida.pdf, [fecha de consulta: 4 de mayo 2018].

Fernández, J. y Fernández, P. (2017). "El derecho a la portabilidad de los datos", en Piñar, J. (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. España: Reus.

Institute of Electrical and Electronics Engineers (IEEE). (1990). *Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*. New York.

Mayer-Schönberger, V. (2009). *Delete: the virtue of forgetting in the digital age*. EE.UU.: Princeton University Press.

Miralles, R. (2012). *El derecho de la portabilidad de los datos personales*. Disponible en: http://www.abogacia.es/2012/11/15/el–derecho–de–la–portabilidad–de–los–datos–personales/

Morgan, P. (2010). *Dictamen del Comité Económico y Social Europeo sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Un enfoque global de la protección de los datos personales en la Unión Europea*. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?toc=OJ%3AC%3A2011%3A248%3ATOC&uri=uriserv%3AOJ.C_.2011.248.01.0123.01.SPA, [fecha de consulta: 4 de mayo 2018].

Peguera, M. (2017). *Propuesta de Reglamento para facilitar la libre circulación de los datos no personales en la UE.* [Mensaje en un blog]. CUATRECASAS. Disponible en: http://blog.cuatrecasas.com/propiedad-intelectual/propuesta-de-reglamento-para-facilitar-la-libre-circulacion-de-los-datos-no-personales-en-la-ue/, [fecha de consulta: 3 de mayo 2018].

Reding, Viviane. 2010. *Building trust in Europe's online single market. Brussels: American Chamber of Commerce to the EU*. Bruselas. Disponible en: http://europa.eu/rapid/press-release_SPEECH-10-327_en.htm.

# TÍTULO CUARTO
# RELACIÓN DEL RESPONSABLE Y ENCARGADO

# CAPÍTULO ÚNICO
# RESPONSABLE Y ENCARGADO

***Artículo 58.*** *El encargado deberá realizar las actividades de tratamiento de los datos personales sin ostentar poder alguno de decisión sobre el alcance y contenido del mismo, así como limitar sus actuaciones a los términos fijados por el responsable.*

***Artículo 59.*** *La relación entre el responsable y el encargado deberá estar formalizada mediante contrato o cualquier otro instrumento jurídico que decida el responsable, de conformidad con la normativa que le resulte aplicable, y que permita acreditar su existencia, alcance y contenido.*

*En el contrato o instrumento jurídico que decida el responsable se deberán prever, al menos, las siguientes cláusulas generales relacionadas con los servicios que preste el encargado:*

*I. Realizar el tratamiento de los datos personales conforme a las instrucciones del responsable;*

*II. Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;*

*III. Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables;*

*IV. Informar al responsable cuando ocurra una vulneración a los datos personales que trata por sus instrucciones;*

*V. Guardar confidencialidad respecto de los datos personales tratados;*

*VI. Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y*

*VII. Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, o la comunicación derive de una subcontratación, o por mandato expreso de la autoridad competente.*

*Los acuerdos entre el responsable y el encargado relacionados con el tratamiento de datos personales no deberán contravenir la presente Ley y demás disposiciones aplicables, así como lo establecido en el aviso de privacidad correspondiente.*

***Artículo 60.*** *Cuando el encargado incumpla las instrucciones del responsable y decida por sí mismo sobre el tratamiento de los datos personales, asumirá el carácter de responsable conforme a la legislación en la materia que le resulte aplicable.*

***Artículo 61.*** *El encargado podrá, a su vez, subcontratar servicios que impliquen el tratamiento de datos personales por cuenta del responsable, siempre y cuando medie la autorización expresa de este último. El subcontratado asumirá el carácter de encargado en los términos de la presente la Ley y demás disposiciones que resulten aplicables en la materia.*

*Cuando el contrato o el instrumento jurídico mediante el cual se haya formalizado la relación entre el responsable y el encargado, prevea que este último pueda llevar a cabo a su vez las subcontrataciones de servicios, la autorización a la que refiere el párrafo anterior se entenderá como otorgada a través de lo estipulado en éstos.*

***Artículo 62.*** *Una vez obtenida la autorización expresa del responsable, el encargado deberá formalizar la relación adquirida con el subcontratado a través de un contrato o cualquier otro instrumento jurídico que decida, de conformidad con la normatividad que le resulte aplicable, y permita acreditar la existencia, alcance y contenido de la prestación del servicio en términos de lo previsto en el presente Capítulo.*

***Artículo 63.*** *El responsable podrá contratar o adherirse a servicios, aplicaciones e infraestructura en el cómputo en la nube, y otras materias que impliquen el tratamiento de datos personales, siempre y cuando el proveedor externo garantice políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la presente Ley y demás disposiciones que resulten aplicables en la materia.*

*En su caso, el responsable deberá delimitar el tratamiento de los datos personales por parte del proveedor externo a través de cláusulas contractuales u otros instrumentos jurídicos.*

***Artículo 64.*** *Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura de cómputo en la nube y otras materias, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor:*

*I. Cumpla, al menos, con lo siguiente:*

*a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la presente Ley y demás normativa aplicable;*

*b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;*

*c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que preste el servicio, y*

*d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio;*

*II. Cuente con mecanismos, al menos, para:*

*a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;*

*b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;*

*c) Establecer y mantener medidas de seguridad para la protección de los datos personales sobre los que se preste el servicio;*

*d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable y que este último haya podido recuperarlos, y*

*e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien, en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.*

*En cualquier caso, el responsable no podrá adherirse a servicios que no garanticen la debida protección de los datos personales, conforme a la presente Ley y demás disposiciones que resulten aplicables en la materia.*

# COMENTARIO

**Miguel Recio Gayo**

## I. Antecedentes

Las figuras del responsable y del encargado del tratamiento son el centro de atención de la normatividad sobre protección de datos personales por lo que se refiere a la adopción e implementación de medidas para su cumplimiento.

El responsable del tratamiento, sobre el que recae la obligación de adoptar medidas técnicas y organizativas para garantizar el derecho humano a la protección de datos personales, y el encargado del tratamiento, que ofrece servicios de tratamiento de los datos personales a aquél y que por tanto tiene que cumplir igualmente con los requisitos de la normatividad sobre protección de datos, quedan vinculados en virtud de un contrato u otro instrumento jurídico que debe establecer, entre otras cuestiones, las obligaciones y responsabilidades en la materia de cada uno de los mismos.

La LGPDPPSO dedica los artículos 58 al 64, del Capítulo Único Responsable y Encargado, correspondiente al Título Cuarto Relación del Responsable y Encargado, al tratamiento de datos personales que el encargado del tratamiento haga por cuenta del responsable del tratamiento.

Es así que el objeto de los presentes comentarios es atender a los antecedentes y definiciones actuales de las figuras del responsable y del encargado del tratamiento, la necesidad de que las relaciones entre ambos, que impliquen la prestación de un servicio de tratamiento de datos personales por el encargado, estén formalizadas a través de un contrato u otro instrumento jurídico, así como a la subcontratación en caso de que se recurra a otro u otros encargados del tratamiento. Además, el uso de servicios de cómputo en la nube plantea que, en particular cuando el responsable del tratamiento se adhiera a condiciones o cláusulas generales de la contratación predispuestas por el prestador de servicios de nube, aquél deba asegurarse de que se garantiza el derecho humano a la protección de datos personales a lo largo de toda la cadena de contratación, por lo que se presta especial atención al mismo.

Por último, se hacen algunas consideraciones adicionales al Capítulo Único objeto de comentario y se presentan las correspondientes conclusiones a las que da lugar el análisis previo.

## II. Relevancia temática y contexto

La primera referencia a nivel nacional a la figura del responsable del tratamiento, aunque no se definió entonces, se encuentra en la abrogada LFTAIPG.[134] En concreto, en su artículo 20 comenzaba indicando que los sujetos obligados, siendo definido dicho concepto a su vez en la fracción XIV del artículo 3, son "responsables de los datos personales" y tienen que cumplir con las obligaciones que se prevén en dicho artículo.

Entre otras obligaciones, los sujetos obligados, como responsables de los datos personales tenían que adoptar procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos, capacitar a los servidores públicos y dar a conocer sus políticas en relación con la protección de datos, así como tratar los datos personales sólo cuando éstos fueran adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hubieran obtenido. Es decir, eran obligaciones propias de un responsable del tratamiento por lo que se refiere a adoptar medidas técnicas y organizativas para proteger los datos personales durante su tratamiento.

Dichas obligaciones de los responsables de los datos personales son relevantes, ya que constituyen también los antecedentes de la actual obligación del responsable del tratamiento y que se extiende también al encargado del tratamiento cuando éste tiene acceso a los datos personales para prestar algún servicio al responsable del tratamiento o dicho servicio consiste, precisamente, en el tratamiento de los datos personales por cuenta de aquél.

Sin perjuicio de lo anterior, una primera definición de las figuras de responsable y encargado del tratamiento se encuentra en los Lineamientos de Protección de Datos Personales.[135] En concreto, conforme a la fracción IV del Lineamiento Tercero, se considera responsable al "servidor público titular de la unidad administrativa designado por el titular de la dependencia o entidad, que decide sobre el tratamiento físico o automatizado de datos personales, así como el contenido y finalidad de los sistemas de datos personales". Y la fracción II del citado Lineamiento define al encargado como "el servidor público o cualquier otra persona física o moral facultado por un instrumento jurídico o expresamente autorizado por el responsable para llevar a cabo el tratamiento físico o automatizado de los datos personales".

Como indica Arias, la clave de estas definiciones está en que el responsable lo es porque decide sobre el tratamiento que se va a llevar a cabo.[136] Esto

[134] Publicada en el *Diario Oficial de la Federación* el 11 de junio de 2002. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/abro/lftaipg/LFTAIPG_abro.pdf.

[135] Publicados en el *Diario Oficial de la Federación* del 30 de septiembre de 2005. Disponible en: http://inicio.inai.org.mx/MarcoNormativoDocumentos/lineamientos_protdaper.pdf.

[136] Arias, M. (2009). *El encargado del tratamiento y el documento de seguridad del responsable del fichero*. [Archivo PDF]. Disponible en: https://www.navarra.es/NR/rdonlyres/E6188543-88F9-476F-

implica, como explica el Grupo de Trabajo del Artículo 29, que "aun cuando la capacidad de 'determinar' se derive de una atribución específica por ley, tal capacidad procede por lo general de un análisis de los elementos de hecho o de las circunstancias del caso: se debe atender a las operaciones concretas del tratamiento en cuestión y ha de comprenderse quién las determina".[137] Y en este sentido, "el encargado del tratamiento debe limitarse a tratar los datos por cuenta del responsable y de acuerdo con sus instrucciones, con respeto escrupuloso a sus instrucciones"[138] lo que significa que el encargado del tratamiento no puede tomar decisión alguna sobre el tratamiento de los datos personales, ya que los trata por cuenta del responsable.

El encargado del tratamiento es un tercero en el sentido de que es una persona u organización separada o distinta al responsable del tratamiento, pero no es un tercero en el sentido de que recibe una transferencia de datos personales lo que supondría que se convirtiese en un nuevo responsable del tratamiento.

Además, cabe resaltar que el encargado del tratamiento no está legitimado, ni contractual ni legalmente, para tratar los datos personales que le ha encomendado el responsable más allá de la prestación del servicio correspondiente, ya sea que dicho servicio implique el acceso a los datos personales o que dicho servicio consista específicamente en el tratamiento de datos personales.

## III. Análisis del contenido

De acuerdo con lo anterior, el artículo 58 de la LGPDPPSO indica claramente que el encargado del tratamiento tratará los datos personales "sin ostentar poder alguno de decisión sobre el alcance y contenido del mismo", de manera que limitará "sus actuaciones a los términos fijados por el responsable". Y en relación con esta cuestión, el artículo 60 indica que si el encargado del tratamiento incumple las instrucciones dadas por el responsable y decide "por sí mismo sobre el tratamiento de los datos personales, asumirá el carácter de responsable conforme a la legislación en la materia que le resulte aplicable".

Dicho tratamiento de datos personales por el encargado del tratamiento sería ilícito, ya que supondría "dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente ley", tal como indica la fracción IV del artículo 163 de la LGPDPPSO. Esta causa de responsabilidad sería considerada, en virtud del artículo mencionado, una infracción grave para efectos de su sanción administrativa.

8581-406069D3C0E7/188890/15PonenciaCongresoDeusto2009.pdf, [fecha de consulta: 4 de mayo 2018].

[137] Grupo de Trabajo del Artículo 29. (2010). *Dictamen 1/2010 sobre los conceptos de responsable del tratamiento y encargado del tratamiento, WP 169*. Adoptado el 16 de febrero, p. 9.

[138] Piñar Mañas & Asociados, S.C. (2013). *Guía para empresas en materia de protección de datos personales en el uso del cómputo en la nube (cloud computing)*. México: Prosoft, p.4.

A escala internacional, y como referencia conveniente para la interpretación de estas figuras, cabe considerar que la figura del responsable del tratamiento tiene su origen en la de *autoridad controladora* que aparece en el Convenio 108 del Consejo de Europa, del 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.[139] Este concepto, como indican Del Conde y Martínez, "fue evolucionando con la finalidad de responder a las necesidades de la vida práctica, hasta llegar a la denominación actual del 'responsable del tratamiento de datos personales'. Este cambio se debe igualmente a un interés genuino por establecer conceptos cada vez más claros que contribuyeran a garantizar una aplicación más eficaz de la normatividad y el cumplimiento en la práctica de los sujetos involucrados".[140]

Sobre la figura del encargado del tratamiento, también a escala internacional y en relación con su inclusión en la Directiva 95/46/CE,[141] Heredero indica que "el concepto de 'encargado del tratamiento' no figuraba en la propuesta de 1990, aun cuando el artículo 22 regulaba el tratamiento de datos por personas distintas del responsable del fichero, pero por cuenta de éste. La enmienda 18 del Parlamento Europeo propuso la inclusión de una definición más específica (que figuraría como apartado e bis) en iguales términos que la enmienda 18. La memoria de la propuesta no explicaba las razones de ello y se limitaba a decir que se trataba de una definición útil".[142]

La LGPDPPSO define, respectivamente en las fracciones XXVIII y XV, al responsable del tratamiento como "los sujetos obligados a los que se refiere el artículo 1 de la presente ley que deciden sobre el tratamiento de los datos personales" y al encargado del tratamiento como "la persona física o jurídica, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras trate datos personales a nombre y por cuenta del responsable".

En cualquier caso, es necesario considerar que, a pesar de la claridad de las definiciones de responsable y encargado del tratamiento, como ha indicado Buttarelli, en muchos casos la distinción entre las mismas se ha vuelto cada vez más compleja y difusa.[143]

---

[139] Disponible en: https://rm.coe.int/16806c1abd.

[140] Del Conde, A. y Martínez, E. (2013). "Sujetos que intervienen en la relación jurídica que se genera derivado del tratamiento de datos personales: caso de responsable, encargado y tercero", en Ornelas, L. y Piñar, J. (Coords.), *La Protección de Datos Personales en México*. México: Editorial Tirant Lo Blanch, p. 147.

[141] 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, publicada en el *Diario Oficial de las Comunidades Europeas* L 281 el 23 de noviembre de 1995.

[142] Heredero, M. (1997). *La Directiva Comunitaria de Protección de Datos de Carácter Personal*. Pamplona, España: Aranzadi, p. 82.

[143] Butarelli, G. (2012). *Security and privacy regulatory challenges in the Cloud, The 2012 European Cloud Computing Making the Transition from Cloud-Friendly to Cloud-Active*. Bruselas. [Archivo PDF]. Disponible en: http://www.feelingeurope.eu/Pages/cloud%20computing%20Buttarelli%20-%20EDPS.pdf

**1. Formalización de la prestación del servicio de tratamiento.** El tratamiento de los datos personales por el encargado es el objeto de la relación que se establece entre éste y el responsable del tratamiento, debiendo formalizarse "mediante contrato o cualquier otro instrumento jurídico que decida el responsable", como indica el artículo 59 de la LGPDPPSO.

Al respecto, el Lineamiento Vigésimo Primero de los Lineamientos de Protección de Datos Personales, relativo al tratamiento de datos por terceros, indicaba que "deberá estipularse en el contrato respectivo, la implementación de medidas de seguridad y custodia previstas en los presentes Lineamientos, en la normatividad aplicable a las dependencias y entidades contratantes, así como la imposición de penas convencionales por su incumplimiento".

El requisito de un contrato o cualquier otro instrumento jurídico se debe, en particular, a la necesidad de poder hacer exigibles las medidas técnicas y organizativas que el responsable haya implementado y que, a través de dicho contrato o instrumento jurídico extienda también al encargado o encargados del tratamiento que tengan acceso a los datos personales.

En el derecho comparado el contrato que regula la relación entre el responsable y el encargado del tratamiento es un requisito exigible para garantizar el cumplimiento de las obligaciones exigibles al responsable y al encargado del tratamiento. Así se indica, por ejemplo, en el artículo 17 de la Directiva 95/46/CE, la cual exige que "la realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento".

Al respecto, dicho artículo "establece la necesidad de que haya un contrato u otro acto jurídico vinculante que regule la relación entre el responsable y el encargado del tratamiento de datos. Dicho contrato debe constar por escrito a efectos de conservación de la prueba y ha de tener un contenido mínimo que establezca, en particular, que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento y contemple medidas técnicas y de organización para proteger adecuadamente los datos personales".[144]

El Reglamento general de protección de datos[145] prevé también en su artículo 28 que el tratamiento de datos personales por el encargado del tratamiento "se regirá por un contrato u otro acto jurídico" que le vinculará jurídicamente con el responsable del tratamiento. Este contrato u otro acto

[144] Véase nota 137.

[145] 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), *Diario Oficial de la Unión Europea,* L 119, 4 de mayo de 2016.

jurídico establecerá "el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable" e incluirá, en particular, las cuestiones que se incluyen en el mencionado artículo y que se refieren, entre otros aspectos, a seguir las instrucciones del responsable del tratamiento referidas también a las transferencias internacionales de datos; la confidencialidad de los datos personales tratados; las medidas de seguridad; la subcontratación; la asistencia al responsable del tratamiento para ayudar a cumplir con sus obligaciones o la devolución o supresión de los datos personales, incluidas las copias existentes en este último caso, a la finalización de los servicios de tratamiento.

Por lo que se refiere al contenido del contrato u otro instrumento jurídico, el artículo 59 de la LGPDPPSO indica cuál será, como mínimo, el contenido del mismo. Dicho artículo sigue, en gran medida, el artículo 50 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[146] relativo a las obligaciones del encargado del tratamiento. En concreto, las cláusulas generales relacionadas con el tratamiento de datos personales por el encargado del tratamiento, que incluye el mencionado artículo de la LGPDPPSO, son las relativas a:

1. Instrucciones para el tratamiento de los datos personales y finalidades:

    1.1 Seguir las instrucciones dadas por el responsable del tratamiento.

    1.2 Abstenerse de tratarlos para las finalidades distintas a las instruidas por el responsable del tratamiento.

2. Medidas de seguridad y confidencialidad:

    2.1 Implementar las medidas de seguridad conforme a los instrumentos jurídicos aplicables.

    2.2 Informar al responsable cuando ocurra una vulneración a los datos personales que trata por instrucciones del responsable del tratamiento.

    2.3 Guardar confidencialidad respecto de los datos personales tratados.

3. Finalización del servicio:

    3.1 Suprimir o devolver los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales.

[146] Disponible en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

4. Transferencia de los datos personales:

4.1 Abstenerse de transferir los datos personales, salvo en el caso de que:

a) el responsable así lo determine,

b) la comunicación derive de una subcontratación o

c) por mandato expreso de la autoridad competente.

El último párrafo del artículo 59 de la LGPDPPSO indica que los acuerdos entre el responsable y el encargado del tratamiento "no deberán contravenir la presente Ley y demás disposiciones aplicables, así como lo establecido en el aviso de privacidad correspondiente". En particular, esta última hace referencia a que el acuerdo no contravenga lo establecido en el aviso de privacidad correspondiente, en el que, entre otros aspectos, se encontraría la finalidad o finalidades del tratamiento de los datos, lo cual implica que sea recomendable adjuntar al contrato u otro instrumento jurídico que formalice la relación jurídica entre el responsable y el encargado del tratamiento, dicho aviso de privacidad o, al menos, una referencia de dónde se encuentra disponible, como una dirección de internet.

Finalmente, en relación con lo anterior es necesario recordar que la remisión de datos personales entre el responsable y el encargado del tratamiento, ni requiere ser informada a la persona cuyos datos personales son tratados, ni requiere su consentimiento.

**2. La subcontratación.** La subcontratación, que se produce cuando el encargado del tratamiento subcontrata todos o parte de los servicios de tratamiento de datos que presta al responsable del tratamiento o que implican el acceso a los datos personales por los subcontratistas, es objeto de los artículos 61 y 62 de la LGPDPPSO.

El primero de estos artículos tiene por objeto la norma general en materia de subcontratación de "servicios que impliquen el tratamiento de datos personales por cuenta del responsable", en virtud de que "siempre y cuando medie la autorización expresa" del responsable del tratamiento, el encargado del tratamiento podrá subcontratarlos. Es decir, para poder subcontratar la totalidad o parte del servicio que implique el tratamiento de datos personales por cuenta del responsable del tratamiento, es necesaria autorización expresa del responsable del tratamiento.

Esta autorización expresa, necesaria para poder subcontratar, se entenderá como otorgada si, como se indica en el párrafo segundo del artículo 61, el contrato u otro instrumento jurídico en el que se formalice la relación jurídica entre el responsable y el encargado del tratamiento "prevea que este último pueda llevar a cabo a su vez

las subcontrataciones de servicios". Cabe señalar que no se especifica nada sobre si dicha autorización expresa puede ser genérica, sin identificar específicamente al encargado del tratamiento por su nombre o denominación social, pudiendo obtenerse por medio de la indicación de la necesidad de subcontratación si fuera necesario, o si se tiene que identificar quién es el encargado del tratamiento concreto que prestará servicios que impliquen el acceso a los datos personales.

La autorización de la subcontratación en el contrato u otro instrumento jurídico, ya sea que se encuentre en soporte electrónico o en papel, permite su prueba por las partes.

En relación con la figura del subcontratista, el artículo 61 indica que "asumirá el carácter de encargado". Este subcontratista es también un encargado del tratamiento que trata datos por cuenta del responsable del tratamiento asumiendo las mismas obligaciones previstas para el encargado del tratamiento inicial.

El segundo de los artículos mencionados se refiere a la obligación de formalizar en un contrato u otro instrumento jurídico la subcontratación. Con esta medida se trata también de extender las obligaciones aplicables al encargado del tratamiento a otros encargados del tratamiento a los que se recurra para el tratamiento de datos por cuenta del responsable del tratamiento.

Si bien el artículo 62 de la LGPDPPSO indica que es el encargado del tratamiento quien "deberá formalizar la relación adquirida con el subcontratado a través de un contrato o cualquier otro instrumento jurídico que decida", dicha decisión tendrá que ser conforme a lo que el responsable del tratamiento determine, ya que si éste puede decidir sobre el instrumento por el que se formalice la relación con el encargado del tratamiento, como se prevé en el artículo 59 de la LGPDPPSO, debe poder hacerlo también en este caso, máxime si se considera que el mismo tendrá que demostrar el cumplimiento con la normatividad sobre protección de datos personales y también tiene la obligación de garantizar el cumplimiento a lo largo de la cadena de contratación con los encargados del tratamiento.

Al igual que en el caso de la relación jurídica entre el responsable y el encargado del tratamiento, el artículo 62 repite que el contrato o cualquier otro instrumento jurídico relativo a la subcontratación deberá permitir "acreditar la existencia, alcance y contenido de la prestación del servicio". Esta exigencia queda justificada por la necesidad de extender con carácter vinculante las medidas técnicas y organizativas, así como en su caso prever la responsabilidad exigible, que se requieren para proteger de manera efectiva los datos personales tanto por el responsable del tratamiento como por cualquier encargado del tratamiento que participe en el tratamiento de los datos personales.

Es importante considerar también que las obligaciones exigibles al encargado del tratamiento y que son objeto del artículo 59 de la LGPDPPSO, se extienden a cualquier otro encargado del tratamiento al que se recurra para el tratamiento de los datos personales. Se explica así la referencia a que el contrato o cualquier otro instrumento jurídico por el que se formalice la subcontratación se haga "en términos de lo previsto en el presente Capítulo", como indica el artículo 62 de la LGPDPPSO.

Por tanto, son dos los requisitos que se aplican a la subcontratación de tratamientos de datos personales por cuenta del responsable. El primero, siendo además condición necesaria para poder aplicar el segundo, es el relativo a la necesidad de autorización expresa por el responsable del tratamiento, entendiéndose otorgada si la misma está prevista en el contrato u otro instrumento jurídico por el que se formalice la relación jurídica entre el responsable y el encargado del tratamiento. Y el segundo es que la relación jurídica que dé lugar a la subcontratación se formalice también a través de un contrato u otro instrumento jurídico.

**3. El cómputo en la nube.** La LGPDPPSO incluye el cómputo en la nube como parte de la relación entre el responsable y el encargado del tratamiento, lo que significa que se considere que dicho tratamiento se realice por el prestador de servicios de nube como encargado del tratamiento por cuenta del cliente, siendo este último el responsable del tratamiento.

Es decir, el cómputo en la nube, cuando implique un tratamiento de datos personales, queda regulado como un tratamiento de datos por un encargado, lo que significa que se contemple como una remisión de datos personales, si bien podrían darse otros casos en los que se produzca una transferencia de datos entre responsables del tratamiento o que tanto el cliente de los servicios de nube como el prestador de dichos servicios sean, respectivamente, responsables del tratamiento.

Al respecto, como se indica en la *Guía para empresas en materia de protección de datos personales en el uso del cómputo en la nube (cloud computing)*, siendo aplicable también a los sujetos obligados en el sector público, "con carácter general desde la perspectiva de la protección de datos personales las partes interesadas en las relaciones de cómputo en la nube tienen la siguiente naturaleza: el usuario tiene la consideración de responsable del tratamiento, el prestador del servicio tiene la consideración de encargado del tratamiento y el subcontratista tiene la consideración de subencargado del tratamiento".[147]

El cómputo en la nube es definido en la fracción VI del artículo 3 de la LGPDPPSO como el "modelo de provisión externa de servicios de cómputo

[147] Piñar Mañas & Asociados S.C. (2013). *Guía para empresas en materia de protección de datos personales en el uso del cómputo en la nube (cloud computing)*. México: Prosoft, p. 141.

bajo demanda, que implica el suministro de infraestructura, plataforma o programa informático, distribuido de modo flexible, mediante procedimientos virtuales, en recursos compartidos dinámicamente" y los artículos 63 y 64 de la LGPDPPSO están dedicados a él.

Tratar datos personales en el cómputo en la nube implica, como señalan Maqueo, Moreno y Recio, que:

> el responsable del tratamiento, en dicha condición y como cliente de los servicios de cómputo en la nube, tiene que ser consciente de cómo y para qué obtiene y trata los datos personales. Esto implica que tenga que adoptar las medidas necesarias para cumplir con los principios, deberes y derechos establecidos en la normatividad, de manera que se minimice el tratamiento de los datos personales, lo que significa también que tenga que conocer quién es el proveedor de servicios de cómputo en la nube al que elige, en su caso, como encargado del tratamiento.[148]

El artículo 63 de la LGPDPPSO, partiendo de que el responsable del tratamiento podrá contratar o adherirse a servicios de cómputo en la nube y otras materias, sin especificar a qué se refiere con esta última referencia, indica que aquél tendrá que asegurarse de que "el proveedor externo garantice políticas de protección de datos personales equivalentes a los principios y deberes establecidos en la presente Ley y demás disposiciones que resulten aplicables en la materia". Es así que los sujetos obligados, al plantearse o al hacer la contratación de servicios de nube tienen que informarse, en particular, de las prácticas del prestador de servicios de nube en materia de protección de datos personales, ya que esto es clave para garantizar el cumplimiento y decidir, en cada caso, sobre las garantías que ofrece dicho prestador.

Y en este sentido, como recomendaciones prácticas, Maqueo, Moreno y Recio, indican que al desarrollar términos de referencia de una licitación pública o procesos de contratación o al evaluar proposiciones en materia de servicios de cómputo en la nube, los responsables del tratamiento deberían considerar, entre otros aspectos, la transparencia en los términos y condiciones de servicio, el centro de datos tecnológico y la geolocalización, las certificaciones que haya obtenido el prestador de servicios de nube, las auditorías de cumplimiento en materia de protección de datos personales y seguridad, la subcontratación de servicios que impliquen el acceso o tratamiento de datos personales, la prohibición de tratar los datos personales con finalidades distintas a la prestación del servicio, la notificación de vulneraciones de seguridad o las métricas de cumplimiento en materia de protección de datos y seguridad.[149]

---

[148] Maqueo, M., Moreno, J. y Recio, M. (2014). *Lineamientos de Protección de Datos en el Cómputo en la nube: Parámetro para su elaboración*. México: CIDE/Microsoft, p. 37.

[149] Maqueo, M., Moreno, J. y Recio, M. (2015). Estándares y recomendaciones para la protección de datos personales en el cómputo en la nube. Su aplicación al caso del Registro Nacional de Víctimas en México. *Revista Juez*, núm. 3, México: Tirant Lo Blanch.

Aunque el artículo 64 de la LGPDPPSO se refiere al caso en el que el responsable del tratamiento hace uso de servicios de la nube, que impliquen el tratamiento de datos personales, a los que se adhiere “mediante condiciones o cláusulas generales de contratación”, sin posibilidad alguna de negociación o modificación, las condiciones previstas en el mismo serían exigibles para cualquier supuesto de contratación de servicios de nube.

Es decir, con independencia de si el uso de los servicios de nube, que impliquen el tratamiento de datos personales por el prestador de servicios de nube como encargado del tratamiento, se haga mediante la negociación de las cláusulas contractuales aplicables o la adhesión a condiciones o cláusulas generales de contratación, el cliente, como responsable del tratamiento, tiene que asegurarse de que el prestador de servicios de nube cumpla y le permita cumplir con las obligaciones que, respectivamente, le son exigibles en materia de protección de datos. Se trata así de que el tratamiento de datos personales que haga el prestador de servicios de nube cumpla con las garantías necesarias para asegurar el cumplimiento de la normatividad mexicana sobre protección de datos personales, ya que de otra manera se podría vulnerar el derecho humano a la protección de datos personales.

Esta obligación de garantizar el derecho humano a la protección de datos personales a lo largo de toda la cadena de contratación en la que participa el encargado del tratamiento y en la que podrían participar también otros encargados del tratamiento (subencargados), da lugar a que el mencionado artículo incluya la prohibición de que el responsable del tratamiento se adhiera a “servicios que no garanticen la debida protección de datos personales, conforme a la presente Ley y demás disposiciones que resulten aplicables en la materia”.

Adoptar medidas técnicas y organizativas para cumplir con la normatividad de protección de datos implica que deban extenderse también a quienes traten datos personales por cuenta del responsable del tratamiento. Y esto determina que la LGPDPPSO, siguiendo a su vez el artículo 52 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, relativo al tratamiento de datos personales en el denominado cómputo en la nube, incluya los requisitos y mecanismos que, como mínimo, son exigibles al prestador de servicios de nube, como encargado del tratamiento. Dicha exigencia tiene como objetivo que el responsable del tratamiento se asegure de que el tratamiento de datos personales que haga el prestador de servicios de nube cumpla con los requisitos en materia de protección de datos previstos en la normatividad sobre protección de datos, con independencia de dónde se tratan los mismos. Así, se facilita que el responsable del tratamiento pueda hacer uso de cualquier prestador de servicios de nube que ofrezca las garantías necesarias para proteger el derecho humano a la protección de datos personales.

**4. Algunas consideraciones adicionales.** El análisis del Título Cuarto, junto con otros artículos de la LGPDPPSO relativos, en particular, a las definiciones de las figuras del responsable y encargado del tratamiento, así como al Título Quinto, que tiene por objeto las comunicaciones de datos personales, incluidas las remisiones de datos, sirve también para plantear algunos comentarios que se exponen a continuación.

Se debería haber considerado la conveniencia de incluir una referencia expresa a los artículos 68 y 71 de la LGPDPPSO, o viceversa.

El primero de estos artículos se refiere a las remisiones internacionales, indicando que cuando se haga remisión de datos personales, el encargado del tratamiento se obliga a "proteger los datos personales conforme a los principios y deberes que establece la presente Ley y las disposiciones que resulten aplicables en la materia". Esta obligación, en la práctica, se articulará a través del correspondiente contrato u otro instrumento jurídico en virtud del que sean exigibles al encargado del tratamiento. Es así que, una referencia expresa en los artículos del Título Cuarto, relativo a la relación del responsable y encargado, a estas remisiones internacionales hubiera facilitado la lectura de la ley o, en su caso, haber considerado la conveniencia de incluir el mencionado artículo en dicho título ya que el mismo tiene por objeto las garantías exigibles por el responsable del tratamiento al encargado del tratamiento, con independencia de dónde se traten los datos personales.

El segundo de los artículos se refiere a que las remisiones de datos personales, tanto nacionales como internacionales, no requieren ser informadas al titular ni contar con su consentimiento. Al igual que en el caso anterior, podría haberse incluido una referencia expresa en el Título Cuarto al artículo 71 o viceversa ya que tiene importantes implicaciones en la relación jurídica entre el responsable y el encargado del tratamiento.

Sin perjuicio de lo anterior, este último artículo permite también plantear si las previsiones sobre la remisión de datos deberían haber sido excluidas de un título que trata también de transferencias de datos personales, ya que la remisión y la transferencia de datos personales son tratamientos distintos y, por tanto, sujetos a condiciones totalmente diferentes. Por ejemplo, la remisión de datos no requiere ser informada ni ser del consentimiento del interesado, lo que sí debería producirse, en el caso de una transferencia para que el interesado sepa a quién se transfieren sus datos personales. Esto significa que la remisión no es una transferencia, lo que implica que el término *comunicación* de datos deba ser explicado para aclarar su significado y alcance.

Por último, de cara al futuro podría plantearse la oportunidad de considerar las figuras de los corresponsables y profundizar sobre la figura del encargado del tratamiento, ya que en algunos casos los límites no quedan claros en la práctica.

## IV. Conclusiones

En virtud de las consideraciones efectuadas previamente, es posible presentar las siguientes conclusiones:

Primera.- La relación entre el responsable y el encargado del tratamiento tiene que constar en un contrato u otro instrumento jurídico que sirva para que el responsable del tratamiento pueda extender al encargado del tratamiento las obligaciones necesarias para cumplir con la normatividad sobre protección de datos personales. La LGPDPPSO incluye cuál será, como mínimo, el contenido de dicho contrato u otro instrumento jurídico.

Segunda.- Como norma general, para que el encargado del tratamiento pueda subcontratar requiere que el responsable del tratamiento le autorice expresamente. Dicha autorización se entenderá otorgada si el contrato u otro instrumento jurídico en el que se formalice la relación jurídica entre el responsable y el encargado del tratamiento así lo prevé. No obstante, es necesario tener en consideración que la LGPDPPSO no especifica si puede tratarse de una autorización genérica o si la previsión en el contrato u otro instrumento por el que se autorice debe ser específica de manera que se identifique quién es el encargado del tratamiento en cada caso.

Tercera.- Al contratar cualquier servicio que implique el acceso a los datos personales o que consista en el tratamiento de datos personales, el responsable del tratamiento tiene que asegurarse de tomar una decisión informada. Es decir, tiene que conocer las prácticas del encargado del tratamiento en materia de protección de datos y asegurarse de que las garantías se cumplan a lo largo de toda la cadena de subcontratación, de manera que siempre se proteja al titular de los datos en su derecho humano a la protección de datos personales.

Cuarta.- Los servicios de cómputo en la nube quedan incluidos entre las disposiciones relativas al responsable y encargado del tratamiento, de manera que el cliente de los servicios de nube es el responsable del tratamiento y el prestador de dichos servicios el encargado del tratamiento. No obstante, podrían darse otros supuestos diferentes, en los que el prestador de servicios también sea responsable del tratamiento.

Quinta.- Hubiera sido conveniente que en este capítulo, relativo a la relación jurídica entre responsable y encargado, se hubiera incluido una referencia expresa a algunos artículos que se incluyen en el capítulo De las Transferencias y Remisiones de Datos Personales o viceversa. Se trata de cuestiones interrelacionadas ya que las remisiones de datos pueden ser tanto nacionales como internacionales, de manera que debería haber referencias expresas entre unos y otros artículos para facilitar la aplicación de la normatividad.

## Referencias

Arias, M. (2009). *El encargado del tratamiento y el documento de seguridad del responsable del fichero*. [Archivo PDF]. Disponible en: https://www.navarra.es/NR/rdonlyres/E6188543-88F9-476F-8581-406069D3C0E7/188890/15PonenciaCongresoDeusto2009.pdf, [fecha de consulta: 4 de mayo 2018].

Butarelli, G. (2012). *Security and privacy regulatory challenges in the Cloud, The 2012 European Cloud Computing Making the Transition from Cloud-Friendly to Cloud-Active*. Bruselas. [Archivo PDF]. Disponible en: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2012/12-03-21_Cloud_computing_EN.pdf

Del Conde, A. y Martínez, E. (2013). "Sujetos que intervienen en la relación jurídica que se genera derivado del tratamiento de datos personales: caso de responsable, encargado y tercero", en Ornelas, L. y Piñar, J. (Coords.), *La Protección de Datos Personales en México*. México: Editorial Tirant Lo Blanch, p. 147.

Grupo de Trabajo del Artículo 29. (2010). *Dictamen 1/2010 sobre los conceptos de responsable del tratamiento y encargado del tratamiento, WP 169*. Adoptado el 16 de febrero, p. 9.

Heredero, M. (1997). *La Directiva Comunitaria de Protección de Datos de Carácter Personal*. Pamplona, España: Aranzadi.

Maqueo, M., Moreno, J. y Recio, M. (2014). *Lineamientos de Protección de Datos en el Cómputo en la nube: Parámetro para su elaboración*. México: CIDE/Microsoft, p. 37.

Maqueo, M., Moreno, J. y Recio, M. (2015). Estándares y recomendaciones para la protección de datos personales en el cómputo en la nube. Su aplicación al caso del Registro Nacional de Víctimas en México. *Revista Juez*, núm. 3, México: Tirant Lo Blanch.

Piñar Mañas & Asociados, S.C. (2013). *Guía para empresas en materia de protección de datos personales en el uso del cómputo en la nube (cloud computing)*. México: Prosoft, p. 4.

# TÍTULO QUINTO
# COMUNICACIONES DE DATOS PERSONALES

# CAPÍTULO ÚNICO
# DE LAS TRANSFERENCIAS Y REMISIONES DE DATOS PERSONALES

***Artículo 65.*** *Toda transferencia de datos personales, sea ésta nacional o internacional, se encuentra sujeta al consentimiento de su titular, salvo las excepciones previstas en los artículos 22, 66 y 70 de esta Ley.*

***Artículo 66.*** *Toda transferencia deberá formalizarse mediante la suscripción de cláusulas contractuales, convenios de colaboración o cualquier otro instrumento jurídico, de conformidad con la normatividad que le resulte aplicable al responsable, que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes.*

*Lo dispuesto en el párrafo anterior, no será aplicable en los siguientes casos:*

*I. Cuando la transferencia sea nacional y se realice entre responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos, o*

*II. Cuando la transferencia sea internacional y se encuentre prevista en una ley o tratado suscrito y ratificado por México, o bien, se realice a petición de una autoridad extranjera u organismo internacional competente en su carácter de receptor, siempre y cuando las facultades entre el responsable transferente y receptor sean homólogas, o bien, las finalidades que motivan la transferencia sean análogas o compatibles respecto de aquéllas que dieron origen al tratamiento del responsable transferente.*

***Artículo 67.*** *Cuando la transferencia sea nacional, el receptor de los datos personales deberá tratar los datos personales, comprometiéndose a garantizar su confidencialidad y únicamente los utilizará para los fines que fueron*

*transferidos atendiendo a lo convenido en el aviso de privacidad que le será comunicado por el responsable transferente.*

***Artículo 68.*** *El responsable sólo podrá transferir o hacer remisión de datos personales fuera del territorio nacional cuando el tercero receptor o el encargado se obligue a proteger los datos personales conforme a los principios y deberes que establece la presente Ley y las disposiciones que resulten aplicables en la materia.*

***Artículo 69.*** *En toda transferencia de datos personales, el responsable deberá comunicar al receptor de los datos personales el aviso de privacidad conforme al cual se tratan los datos personales frente al titular.*

***Artículo 70.*** *El responsable podrá realizar transferencias de datos personales sin necesidad de requerir el consentimiento del titular, en los siguientes supuestos:*

*I. Cuando la transferencia esté prevista en esta Ley u otras leyes, convenios o Tratados Internacionales suscritos y ratificados por México;*

*II. Cuando la transferencia se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;*

*III. Cuando la transferencia sea legalmente exigida para la investigación y persecución de los delitos, así como la procuración o administración de justicia;*

*IV. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente, siempre y cuando medie el requerimiento de esta última;*

*V. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios, siempre y cuando dichos fines sean acreditados;*

*VI. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular;*

*VII. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;*

*VIII. Cuando se trate de los casos en los que el responsable no esté obligado a recabar el consentimiento del titular para el tratamiento y transmisión de sus datos personales, conforme a lo dispuesto en el artículo 22 de la presente Ley, o*

*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.*

***Artículo 71.*** *Las remisiones nacionales e internacionales de datos personales que se realicen entre responsable y encargado no requerirán ser informadas al titular, ni contar con su consentimiento.*

## COMENTARIO

**María Mercedes Albornoz**

### I. Antecedentes

La regulación de las comunicaciones de datos personales en México halla su antecedente más antiguo de fuente interna en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental de 2002[150] (abrogada en 2016[151]). Ésta establecía un marco general con respecto a la protección de datos personales y su transmisión. Los sujetos obligados debían adoptar las medidas necesarias para garantizar la seguridad de los datos personales y evitar su transmisión no autorizada (artículo 20, VI). Se prohibía la difusión, distribución o comercialización de datos personales, salvo que se contara con el consentimiento expreso de los individuos a quienes la información hiciera referencia (artículo 21). Finalmente, se establecía una serie de excepciones al consentimiento como requisito para la transmisión de datos personales (artículo 22).

Avanzando en el tiempo encontramos un instrumento emitido por el Instituto Federal de Acceso a la Información (IFAI) en el año 2005: los Lineamientos de Protección de Datos Personales.[152] Dichos lineamientos, dirigidos a la Administración Pública Federal, desarrollan con mayor profundidad la protección de datos personales. Contienen definiciones, principios y, en lo atinente a la transmisión de datos personales, el concepto y un capítulo completo (el IV) en el que se contempla la transmisión de datos personales con o sin consentimiento del titular y el informe o notificación al titular. De acuerdo

[150] Publicada en el *Diario Oficial de la Federación* el 11 de junio de 2002. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/abro/lftaipg/LFTAIPG_abro.pdf.

[151] La ley de 2002 fue abrogada por una nueva Ley Federal de Transparencia y Acceso a la Información Pública, publicada en el *Diario Oficial de la Federación* el 9 de mayo de 2016. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/lftaip/LFTAIP_orig_09may16.pdf

[152] Instituto Federal de Acceso a la Información y Protección de Datos. (2005). *Lineamientos de Protección de Datos Personales*.[Archivo PDF]. Disponible en: http://inicio.ifai.org.mx/MarcoNormativoDocumentos/lineamientos_protdaper.pdf, [fecha de consulta: 5 de mayo 2018].

con el lineamiento tercero, fracción IV, se entiende por *transmisión*:

> Toda entrega total o parcial de sistemas de datos personales realizada por las dependencias y entidades a cualquier persona distinta al Titular de los datos, mediante el uso de medios físicos o electrónicos tales como la interconexión de computadoras, interconexión de bases de datos, acceso a redes de telecomunicación, así como a través de la utilización de cualquier otra tecnología que lo permita.

Posteriormente, en el año 2009 hubo un par de reformas a la CPEUM que incidieron en la protección de los datos personales en el país. En primer lugar, la reforma del 30 de abril que agregó, entre las facultades del Congreso de la Unión, la de legislar en materia de protección de datos personales en posesión de particulares (artículo 73, fracción XXIX-O). En segundo lugar, la reforma del 1º de junio del mismo año dio un paso trascendental al añadir un segundo párrafo al artículo 16, en el que se consagró el derecho a la protección de sus datos personales concebido como derecho fundamental y fueron incorporados los derechos ARCO, en los siguientes términos:

> 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.

Cabe destacar que los supuestos de excepción previstos en esta norma constitucional, hallan su correlato en las excepciones a la exigencia de consentimiento del titular para realizar transferencias de sus datos personales, contempladas en el artículo 70 de la reciente LGPDPPSO, que fue publicada en el *Diario Oficial de la Federación* el 26 de enero de 2017.[153]

El 5 de julio de 2010, en consonancia con las reformas constitucionales del año anterior, se expidió la LFPDPPP,[154] que regula la actividad de los particulares (personas físicas o morales) de carácter privado que lleven a cabo el tratamiento de datos personales (artículo 2). Contiene una serie de definiciones, entre las cuales destacamos la de *transferencia*, entendida como "toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento" (artículo 3). Asimismo, la LFPDPPP regula específicamente la transferencia de datos personales, a la cual dedica el capítulo V, conformado por los artículos 36 y 37. Se establece que en las transferencias nacionales y en las internacionales, el responsable que las

[153] Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf.
[154] Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf.

realice a sujetos distintos del encargado debe comunicarles a ellos el aviso de privacidad y las finalidades a las que el titular sujetó el tratamiento de sus datos personales. La aceptación de dicho aviso por parte del tercero receptor implica que éste asume las mismas obligaciones que el responsable. Finalmente, se prevé una serie de excepciones a la regla según la cual toda transferencia nacional o internacional de datos personales requiere, para llevarse a cabo, el consentimiento del titular de tales datos.

Transcurrido un año y medio desde la publicación de la emisión de la LFPDPPP, vio la luz su Reglamento.[155] En éste, la terminología jurídica alcanza un mayor grado de tecnicismo y precisión. Así, por ejemplo, se introduce el término *remisión*, para aludir a "la comunicación de datos personales entre el responsable y el encargado, dentro o fuera del territorio mexicano" (artículo 2, IX). Adicionalmente, se establece que las remisiones nacionales o internacionales de datos personales no requerirán el consentimiento del titular de dichos datos ni le deberán ser informadas (artículo 53); esto se debe a que, al fin y al cabo, el encargado trata los datos por cuenta del responsable. Diferente es el régimen de las transferencias de datos personales previsto en la LFPDPPP y reforzado por el capítulo IV del Reglamento (artículos 67 a 76), mediante algunas disposiciones generales y otras más específicas, aplicables a las transferencias nacionales o a las internacionales. Entre las disposiciones generales contenidas en el Reglamento, señalamos especialmente dos. En primer lugar, la que reafirma la regla, implícita ya en la LFPDPPP, de que toda transferencia, nacional o internacional requiere el consentimiento del titular de los datos personales a transferir (salvo los supuestos excepcionales del artículo 37 de la ley) y de que, además, es necesario informarle la transferencia al titular mediante el aviso de privacidad y ceñirse a la finalidad que la justifica (artículo 68). Asimismo, en segundo lugar, merece ser destacada la disposición que se refiere a las transferencias de datos personales dentro del mismo grupo societario del responsable y que permite el empleo de normas internas de protección de datos personales, de carácter vinculante, si éstas cumplen con la LFPDPPP, el Reglamento y demás normativa aplicable (artículo 70).

Luego, el 7 de febrero de 2014, hubo otra reforma a la Constitución[156] que generó un cambio institucional en materia de datos personales. Dicho cambio también tuvo consecuencias en el área de transparencia, donde produjo cambios realmente sustanciales. Se estableció la autonomía constitucional del órgano garante del derecho de acceso a la información pública y a la protección

[155] Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 21 de diciembre de 2011. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

[156] Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, *Diario Oficial de la Federación,* 7 de febrero de 2014. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_215_07feb14.pdf

de datos personales (artículo 6º, CPEUM), independiente de los poderes Ejecutivo, Legislativo y Judicial. También se facultó al Congreso de la Unión para expedir leyes generales en materia de transparencia gubernamental, acceso a la información y protección de datos personales en posesión de las autoridades, entidades, órganos y organismos gubernamentales de todos los niveles de gobierno (artículo 73, XXIX-S, CPEUM).

El antecedente legislativo más reciente de la ley general data de mayo de 2016. Se trata de la nueva Ley Federal de Transparencia y Acceso a la Información Pública[157] que abrogó la de 2002. Esta nueva ley establece algunas previsiones para que el INAI, como organismo autónomo facultado para regular y resolver asuntos en esta materia, garantice el derecho a la protección de los datos personales.

## II. Relevancia temática y contexto

La comunicación de datos personales es un tema clave en materia de protección de dichos datos, ya que cuando son comunicados de un sujeto obligado a otro, aumentan los riesgos de afectación o vulneración para el titular. A su vez, el tratamiento automatizado y masivo de datos personales, facilitado por las tecnologías de la información y de la comunicación desde hace varias décadas, incrementa más los riesgos, en comparación con épocas previas cuando el tratamiento de datos se llevaba a cabo en forma manual. Pero es a partir de la década de los noventa del siglo XX, con la popularización de Internet y su utilización para fines comerciales, cuando el problema alcanza una relevancia exponencial que sigue incrementándose en la actualidad, gracias a la frecuente utilización de redes sociales y plataformas en línea que ofrecen distintos tipos de servicios. En efecto, dado que los datos personales del titular se encuentran a tan sólo un clic de distancia de participar en el flujo nacional o incluso transfronterizo de información, los riesgos de vulneración que esto conlleva son cada vez más importantes.

A fin de contextualizar el tema dentro de la LGPDPPSO, se ha de tener presente que tanto la comunicación, como la difusión, la divulgación y la transferencia de datos personales son consideradas *tratamiento* de dichos datos (artículo 3, XXXIII). Estas operaciones de tratamiento quedan comprendidas en el término genérico *comunicaciones* de datos personales. La ley en comento dedica su Título Quinto a las Comunicaciones de Datos Personales, apartado compuesto por un Capítulo Único, titulado De las Transferencias y Remisiones de Datos Personales, que será analizado a continuación.

[157] Ley Federal de Transparencia y Acceso a la Información Pública, publicada en el *Diario Oficial de la Federación* el 9 de mayo de 2016. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/lftaip/LFTAIP_orig_09may16.pdf

## III. Análisis del contenido

En la LGPDPPSO, las comunicaciones de datos personales comprenden dos especies de operaciones: las transferencias y las remisiones de datos personales. Tanto unas como otras pueden ser nacionales o internacionales.

Para distinguir las transferencias de las remisiones es preciso retomar las nociones de responsable y encargado, en los términos de la ley. *Responsable* es cualquiera de los sujetos obligados que decide sobre el tratamiento de datos personales (artículo 3, XVIII). En el ámbito de aplicación de esta ley, son sujetos obligados "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" (artículo 1, párrafo 5º). En cambio, *encargado* es cualquier persona (física o jurídica, pública o privada) ajena a la organización del responsable que, sola o conjuntamente con otras, trate datos personales en nombre y por cuenta del responsable (artículo 3, XV). Por lo tanto, mientras el responsable es, en términos generales, una autoridad o sujeto de carácter público que tiene poder de decisión sobre el tratamiento de datos personales, el encargado es otra persona que no pertenece a la organización del responsable y que lleva a cabo el tratamiento de datos personales; pero no lo hace en nombre propio, sino en nombre y por cuenta del responsable. Esto significa que si en el tratamiento realizado por el encargado se produce una vulneración a los datos personales del *titular* (persona física a quien corresponden los datos personales, artículo 3, XXXI), la responsabilidad recae en cabeza del responsable. Será este último el sancionado por la autoridad competente y luego podrá ejercer el derecho de repetición contra el encargado.

Una vez aclarada la diferencia entre responsable y encargado, podemos introducir las nociones de transferencia y remisión. Ambas son comunicaciones de datos personales y ambas pueden suceder dentro o fuera del territorio mexicano (lo que determinará su carácter de nacionales o internacionales). La distinción se da en virtud de los sujetos intervinientes: la transferencia la realiza el responsable "a persona distinta del titular, del responsable o del encargado" (artículo 3, XXXII); la remisión, en cambio, es la "comunicación de datos personales realizada exclusivamente entre el responsable y encargado" (artículo 3, XVIII). Por ejemplo, son remisiones y no transferencias: la comunicación de datos personales por parte de un partido político a un *call-center* para que se contacte a los ciudadanos a fin de difundir el perfil de sus candidatos, el hecho de que el partido suba datos personales de sus afiliados a la nube para conservarlos allí, o la operación del partido político que recurre a la tercerización, subcontratación u *outsourcing* para el tratamiento de datos personales de sus simpatizantes, con la finalidad de analizarlos y clasificarlos según diversos criterios. En estos casos, los sujetos (probablemente personas

morales de carácter privado) que prestan los servicios de *call-center*, de cómputo en la nube o de análisis de datos, actúan en nombre y por cuenta del partido político, que es el responsable del tratamiento.

La transferencia de datos personales se da entre responsables. Por eso entendemos que cuando la definición legal de transferencia establece que la realiza el responsable a persona distinta del responsable, bien podría haber indicado "a persona distinta de sí mismo". Dadas las obligaciones que en una transferencia asume el sujeto receptor, éste también se convierte en responsable. En consecuencia, es posible hablar de un "responsable transferente" y un "responsable receptor".

Del concepto *transferencia* quedan excluidas las comunicaciones de datos personales entre el responsable y el titular de los mismos, así como aquellas que tengan lugar entre responsable y encargado. Estas últimas, como ya se señaló, son remisiones.

Ahora bien, ¿por qué es importante conocer la diferencia entre una transferencia y una remisión de datos personales? o, en otros términos, ¿qué importancia práctica reviste tal distinción? La respuesta la hallamos en el régimen que la LGPDPPSO establece para cada una de ellas. El legislador ha desarrollado con un mayor grado de detalle el régimen de las transferencias; pero también ha contemplado el de las remisiones. Todo gira aquí en torno al consentimiento. Si un responsable va a comunicar datos personales a otra persona, debe actuar con suma diligencia para obtener el consentimiento que necesite, en los términos exigidos.

La regla general en materia de transferencias de datos personales es que están sujetas al consentimiento del titular (artículo 65). Tanto si son nacionales como si son internacionales. En cambio, las remisiones no requieren ser informadas al titular de los datos personales y tampoco precisan contar con su consentimiento (artículo 71). Esta es la diferencia más destacable entre los regímenes jurídicos de estos dos tipos de comunicaciones de datos personales regulados por la LGPDPPSO.

La exigencia del consentimiento del titular en las transferencias es una regla que presenta excepciones. Según el artículo 65, tales excepciones son las previstas en los artículos 22, 66 y 70 de la ley. En efecto, los artículos 22 y 70 contienen supuestos en los cuales el responsable no está obligado a recabar el consentimiento del titular para el tratamiento de sus datos personales (ya hemos visto que la transferencia implica tratamiento), en el primer caso, o para realizar transferencias, en el segundo caso. Sin embargo, llama la atención la inclusión del artículo 66 en la parte final del artículo 65. Porque, aunque el artículo 66 contiene excepciones, se trata de excepciones a otra regla aplicable

a las transferencias: la de su formalización mediante un instrumento jurídico "que permita demostrar el alcance del tratamiento de los datos personales, así como las obligaciones y responsabilidades asumidas por las partes".

Si regresamos a las excepciones a la regla del consentimiento del titular para que sus datos sean transferidos, se advierte una coincidencia entre muchas de las fracciones del artículo 22 y otras tantas del artículo 70. Ambas normas se complementan entre sí y también con la última parte del artículo 16 de la CPEUM. A fin de no generar dudas, el legislador ha incluido por referencia en el artículo 70 (VIII) todos los supuestos excepcionales previstos en el artículo 22. Otras excepciones contempladas en el artículo 70 incluyen la necesidad de realizar una transferencia, sin que sea preciso recabar el consentimiento del titular, por distintos motivos: por razones de seguridad nacional (IX), por virtud de un contrato celebrado o por celebrar en interés del titular por parte del responsable y un tercero (VII), para el cumplimiento de una relación jurídica entre el responsable y el titular (VI), para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, el tratamiento médico o la gestión de servicios sanitarios (V), para el reconocimiento, ejercicio o defensa de un derecho ante autoridad competente (IV), para la investigación y persecución de delitos y para la procuración o administración de justicia (III). También se podrá realizar una transferencia sin requerir el consentimiento del titular cuando esté prevista en alguna ley o tratado internacional del que México sea parte (I), o cuando "se realice entre responsables, siempre y cuando los datos personales se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales" (II).

Otra regla en materia de transferencias de datos personales es que se las debe formalizar mediante un instrumento jurídico suscripto de conformidad con las normas aplicables al responsable (artículo 66, primer párrafo). Allí se establecerán los derechos y obligaciones de las partes, así como el alcance del tratamiento de los datos personales o la finalidad que lo motivó. Este último elemento es importante, porque eventualmente permitirá deslindar responsabilidades en caso de controversia.

La segunda regla aplicable a las transferencias que se acaba de mencionar consta de dos excepciones contenidas en el segundo párrafo del artículo 66. Así, una transferencia no requerirá ser formalizada en los términos del primer párrafo del artículo 66, si es nacional, cuando "se realice entre responsables en virtud del cumplimiento de una disposición legal o en el ejercicio de atribuciones expresamente conferidas a éstos" (I); y si se trata de una transferencia internacional: a) si está prevista en ley o en tratado del que México sea parte, o b) si se realiza "a petición de una autoridad extranjera u organismo internacional competente en carácter de receptor", en este último supuesto, siempre que: i. las facultades entre responsable transferente y

receptor sean homólogas, o ii. “las finalidades que motivan la transferencia sean semejantes o compatibles con las que originaron el tratamiento” de datos por parte del responsable transferente (II).

Además del instrumento jurídico a ser suscrito por el transferente y el receptor, hay otro más que incide en las transferencias de datos personales: el aviso de privacidad. La LGPDPPSO define el aviso de privacidad como el “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”. Este aviso generado por el responsable debe serle comunicado al receptor en toda transferencia de datos personales (artículo 69), a fin de permitir que se respete el principio de finalidad (artículos 16 y 18). Efectivamente, se establece que en una transferencia nacional, el receptor “deberá tratar los datos personales, comprometiéndose a garantizar su confidencialidad y únicamente los utilizará para los fines [para los cuales] (…) fueron transferidos[,] atendiendo a lo convenido en el aviso de privacidad” (artículo 67).

Cuando un responsable establecido en México desea hacer una transferencia o una remisión de datos personales a un receptor o a un encargado que se encuentre fuera del territorio mexicano, la legalidad de la operación (desde la perspectiva de la legislación nacional) está condicionada a que ese tercer receptor o encargado “se obligue a proteger los datos personales conforme a los principios y deberes que establece la presente ley y las disposiciones que resulten aplicables en la materia” (artículo 68).

La internacionalidad de una transferencia o remisión de datos personales, en el marco de la ley analizada en este libro, está dada por el hecho de que el responsable que transferirá o remitirá los datos sea un sujeto obligado mexicano (no olvidemos que se trata de una autoridad mexicana, obviamente establecida en México) y el receptor o encargado destinatario de la comunicación, independientemente de su nacionalidad, sea una persona domiciliada (si es una persona física) o establecida (en caso de ser una persona moral) en el extranjero. Por supuesto que, en el caso inverso, si los datos personales fluyen desde el exterior hacia México, la comunicación también será internacional. Sin embargo, el legislador mexicano concentra sus esfuerzos en regular las comunicaciones internacionales salientes. Esto se explica porque, ante todo, debe garantizar la protección de los datos personales de las personas físicas que se encuentran domiciliadas en México.

El sistema que la LGPDPPSO ha elegido —para brindar seguridad y mecanismos de protección a los titulares— tiene la virtud de la practicidad, especialmente si se lo compara con el sistema aplicable en Europa hasta

el 24 de mayo de 2018 que, como regla general, requería una decisión de adecuación del país de destino, en el sentido de que éste proveyera un nivel de protección adecuado, sustancialmente equivalente al vigente en Europa (ver artículo 25 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo del 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,[158] ver también artículo 45 del Reglamento General de Protección de Datos).[159] Nótese que el artículo 68 de la ley en comento concuerda con la norma del primer párrafo del artículo 66 del mismo cuerpo legal, en lo atinente a las transferencias (en este caso, las internacionales) y su formalización. Ambas disposiciones se refieren al mismo instrumento jurídico, sólo que el artículo 68 precisa que el receptor de la transferencia internacional está obligado a respetar los principios y deberes establecidos en la legislación mexicana.

Finalmente, cuando la comunicación internacional de datos personales es una remisión, surge del artículo 68 la necesidad de que aquí también exista un instrumento jurídico en virtud del cual el encargado se obligue a cumplir con los principios establecidos en la legislación mexicana relativa a la protección de datos personales.

## IV. Conclusiones

La protección de los datos personales de las personas físicas titulares de los mismos adquiere especial importancia cuando tales datos son objeto de comunicación, puesto que el flujo incrementa el riesgo de vulneraciones. La LGPDPPSO se ocupa de esta situación, para lo cual contempla dos grandes tipos de comunicaciones de datos personales y establece un régimen diferenciado para cada una de ellas. De este modo, como regla general, las transferencias requieren el consentimiento del titular, mientras que las remisiones no precisan su consentimiento ni que se le informen a aquél las remisiones de sus datos personales. Adicionalmente, las transferencias deben formalizarse en un instrumento jurídico donde consten el alcance del tratamiento de los datos, las obligaciones y las responsabilidades del responsable transferente y del responsable receptor. En cambio, las remisiones no requieren ser formalizadas en un instrumento con tal contenido.

A su vez, tanto las transferencias como las remisiones pueden ser de carácter nacional o internacional. En el supuesto de transferencias o remisiones internacionales, el legislador ha contemplado las comunicaciones de datos personales que salen del territorio nacional hacia otros países.

[158] Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=ES

[159] Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES Este Reglamento, que entrará en vigor el 25 de mayo de 2018, en los artículos 46 y 47 regula las excepciones a la regla del nivel adecuado con más precisión que la Directiva e incorpora, para los casos de empresas, las normas corporativas vinculantes como mecanismo de autorregulación.

La preocupación subyacente es la de garantizar la protección de los datos más allá de las fronteras de México. Existen, no obstante, limitaciones de competencia territorial al respecto. Ante la desconfianza acerca del tratamiento que podrían recibir los datos personales en el exterior, se parte del supuesto de que las comunicaciones hacia otros países están prohibidas, a menos que el destinatario (tercero responsable receptor o encargado) se obligue a proteger los datos personales que le sean transmitidos, de conformidad con los principios y deberes establecidos por la legislación mexicana aplicable.

## Referencias

DOF. (2002). Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, *Diario Oficial de la Federación*.

DOF. (2011). Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación*.

DOF. (2014). Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, *Diario Oficial de la Federación*. [Archivo PDF]. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_215_07feb14.pdf, [fecha de consulta: 8 de mayo 2018).

DOF. (2016). Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, *Diario Oficial de la Federación*.

Instituto Federal de Acceso a la Información y Protección de Datos. (2005). Lineamientos de Protección de Datos Personales, *Diario Oficial de la Federación*.

Parlamento Europeo y del Consejo. (1995). Directiva 95/46/CE 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, *Diario Oficial de las Comunidades Europeas*. [Archivo PDF]. Disponible en: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31995L0046&from=ES, [fecha de consulta: 8 de mayo 2018).

Parlamento Europeo y del Consejo (2016). Reglamento (UE) 2016/679 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), *Diario Oficial de la Unión Europea*.

# TÍTULO SEXTO

# ACCIONES PREVENTIVAS EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

# CAPÍTULO I
# DE LAS MEJORES PRÁCTICAS

***Artículo 72.*** *Para el cumplimiento de las obligaciones previstas en la presente Ley, el responsable podrá desarrollar o adoptar, en lo individual o en acuerdo con otros responsables, encargados u organizaciones, esquemas de mejores prácticas que tengan por objeto:*

*I. Elevar el nivel de protección de los datos personales;*

*II. Armonizar el tratamiento de datos personales en un sector específico;*

*III. Facilitar el ejercicio de los derechos ARCO por parte de los titulares;*

*IV. Facilitar las transferencias de datos personales;*

*V. Complementar las disposiciones previstas en la normatividad que resulte aplicable en materia de protección de datos personales, y*

*VI. Demostrar ante el Instituto o, en su caso, los Organismos garantes, el cumplimiento de la normatividad que resulte aplicable en materia de protección de datos personales.*

***Artículo 73.*** *Todo esquema de mejores prácticas que busque la validación o reconocimiento por parte del Instituto o, en su caso, de los Organismos garantes deberá:*

*I. Cumplir con los parámetros que para tal efecto emitan, según corresponda, el Instituto y los Organismos garantes conforme a los criterios que fije el primero, y*

*II. Ser notificado ante el Instituto o, en su caso, los Organismos garantes de conformidad con el procedimiento establecido en los parámetros señalados en la fracción anterior, a fin de que sean evaluados y, en su caso, validados o reconocidos e inscritos en el registro al que refiere el último párrafo de este artículo.*

*El Instituto y los Organismos garantes, según corresponda, deberán emitir las reglas de operación de los registros en los que se inscribirán aquellos esquemas de mejores prácticas validados o reconocidos. Los Organismos garantes, podrán inscribir los esquemas de mejores prácticas que hayan reconocido o validado en el registro administrado por el Instituto, de acuerdo con las reglas que fije este último.*

***Artículo 74.*** *Cuando el responsable pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio y de conformidad con esta Ley impliquen el tratamiento intensivo o relevante de datos personales, deberá realizar una Evaluación de impacto en la protección de datos personales, y presentarla ante el Instituto o los Organismos garantes, según corresponda, los cuales podrán emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales.*

*El contenido de la evaluación de impacto a la protección de datos personales deberá determinarse por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.*

***Artículo 75.*** *Para efectos de esta Ley se considerará que se está en presencia de un tratamiento intensivo o relevante de datos personales cuando:*

*I. Existan riesgos inherentes a los datos personales a tratar;*

*II. Se traten datos personales sensibles, y*

*III. Se efectúen o pretendan efectuar transferencias de datos personales.*

***Artículo 76.*** *El Sistema Nacional podrá emitir criterios adicionales con sustento en parámetros objetivos que determinen que se está en presencia de un tratamiento intensivo o relevante de datos personales, de conformidad con lo dispuesto en el artículo anterior, en función de:*

*I. El número de titulares;*

*II. El público objetivo;*

*III. El desarrollo de la tecnología utilizada, y*

*IV. La relevancia del tratamiento de datos personales en atención al impacto social o, económico del mismo, o bien, del interés público que se persigue.*

***Artículo 77.*** *Los sujetos obligados que realicen una Evaluación de impacto en la protección de datos personales, deberán presentarla ante el Instituto o los Organismos garantes, según corresponda, treinta días anteriores a la fecha en*

*que se pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología, ante el Instituto o los organismos garantes, según corresponda, a efecto de que emitan las recomendaciones no vinculantes correspondientes.*

***Artículo 78.*** *El Instituto y los Organismos garantes, según corresponda, deberán emitir, de ser el caso, recomendaciones no vinculantes sobre la Evaluación de impacto en la protección de datos personales presentado por el responsable.*

*El plazo para la emisión de las recomendaciones a que se refiere el párrafo anterior será dentro de los treinta días siguientes contados a partir del día siguiente a la presentación de la evaluación.*

***Artículo 79.*** *Cuando a juicio del sujeto obligado se puedan comprometer los efectos que se pretenden lograr con la posible puesta en operación o modificación de políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales o se trate de situaciones de emergencia o urgencia, no será necesario realizar la Evaluación de impacto en la protección de datos personales.*

## COMENTARIO

**José Luis Piñar Mañas**

### I. Antecedentes

Los sujetos obligados tienen que demostrar el cumplimiento en materia de protección de datos personales y tienen la oportunidad de elevar el nivel establecido por la normativa a través de acciones preventivas como los esquemas de mejores prácticas y de la evaluación de impacto en la protección de datos personales.

Las mejores prácticas en materia de protección de datos personales pueden entenderse como medidas que, tanto los sujetos obligados como el INAI y los organismos garantes, pueden adoptar para dar cumplimiento al objetivo de “promover, fomentar y difundir una cultura de protección de datos personales” previsto en la fracción VII del artículo 2 de la LGPDPPSO.

Estas mejores prácticas de protección de datos personales, que son objeto del Título Sexto de la LGPDPPSO, y a las que se dedican los artículos 72 a 79 de la misma, son acciones preventivas cuyo objeto es elevar el nivel de cumplimiento en la materia por los sujetos obligados e impulsar una cultura sobre protección de datos personales.

Al respecto, el comisionado presidente del INAI, al comentar la última versión de la iniciativa que posteriormente dio lugar a la LGPDPPSO, se adelantó y se refirió a esta última como "la base normativa indicada para que, a partir de la misma, sea posible forjar la tan necesitada cultura de la protección de datos en México".[160] En otras ocasiones he resaltado la importancia de fomentar la cultura de protección de datos.[161]

El objeto de estos comentarios es atender, en particular, algunos antecedentes y referencias relevantes que sirven para poder comprender el alcance y significado de las mejores prácticas en protección de datos personales.

Los comentarios se centran en tres cuestiones relevantes, que son las relativas a los esquemas de mejores prácticas en protección de datos personales: el concepto de tratamiento intensivo o relevante de datos personales y la evaluación de impacto en la protección de datos personales. Además, se incluyen algunas consideraciones adicionales que son resultado del análisis y los comentarios previos.

Por último, se incluyen las correspondientes conclusiones a las que dan lugar los comentarios al articulado que integra el Título Sexto de la LGPDPPSO.

## II. Relevancia temática y contexto

Las mejores prácticas son una de las novedades que introduce la LGPDPPSO, ya que, ni la abrogada LFTAIPG,[162] ni los Lineamientos de Protección de Datos Personales[163] incluían estas acciones preventivas.

Esto supone que, a diferencia de lo que ya ocurría con la normatividad para el sector privado, es una novedad que la LGPDPPSO se refiera a estas mejores prácticas que consisten, por una parte, en la elaboración o adopción de esquemas de mejores prácticas en protección de datos personales y, por otra parte, en la evaluación del impacto.

En concreto, y de manera comparativa, en el caso de los tratamientos de datos personales en el sector privado, la LFPDPPP[164] se refiere en el artículo 44 a la posibilidad de que, tanto las personas físicas como morales, ya sean

[160] Acuña, F. (2016). "La protección de datos personales y notas sobre los desafíos de Internet" en Recio, M. (Coord.), *La Constitución en la sociedad y economía digitales: Temas selectos de derecho digital mexicano*. México: Centro de Estudios Constitucionales, Suprema Corte de Justicia de la Nación, p. 34.

[161] Piñar, J. (2015). "Normalizar la cultura de la protección de datos", en *Veinte años de protección de datos en España*. Madrid, España: Agencia Española de Protección de Datos, p. 81.

[162] Abrogada por los artículos único y transitorio segundo de la Ley Federal de Transparencia y Acceso a la Información Pública, publicada en el *Diario Oficial de la Federación* de 9 de mayo de 2016. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_270117.pdf

[163] Disponible en: http://inicio.inai.org.mx/MarcoNormativoDocumentos/lineamientos_protdaper.pdf

[164] Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

responsables o encargados del tratamiento, puedan "convenir entre ellas o con organizaciones civiles o gubernamentales, nacionales o extranjeras, esquemas de autorregulación vinculante en la materia, que complementen lo dispuesto por la presente Ley" y también a que dichos esquemas de autorregulación puedan consistir en "códigos deontológicos o de buena práctica profesional, sellos de confianza u otros mecanismos y contendrán reglas o estándares específicos que permitan armonizar los tratamientos de datos efectuados por los adheridos y facilitar el ejercicio de los derechos de los titulares". Se trata, por tanto, de un claro referente de los esquemas de mejores prácticas en protección de datos para el sector público. De este modo se pone de manifiesto la importancia que debe darse a la elaboración de códigos de conducta o esquemas de autorregulación, que cada vez adquieren mayor relevancia en el ámbito del derecho y la actividad económica.[165]

En cuanto a la evaluación de impacto en la protección de datos personales, hay que recordar también que el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[166] —aunque no utiliza expresamente el término evaluación de impacto relativo a la protección de datos— en la fracción V del artículo 48 incluye como una medida para garantizar el principio de responsabilidad la relativa a "instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos".

Sin perjuicio de lo anterior, en el caso de las evaluaciones de impacto en la protección de datos personales, es necesario considerar que el sector público sí cuenta ya con experiencia en la materia en el ámbito federal.

En concreto, cabe mencionar, por una parte, las recomendaciones que en 2009 el IFAI (ahora INAI)[167] hizo al anteproyecto de Norma Oficial Mexicana denominada NOM-024-SSA3-2007 que establece los objetivos funcionales y funcionalidades que deberán observar los productos de Sistemas de Expediente Clínico Electrónico para garantizar la interoperabilidad, procesamiento, interpretación, confidencialidad, seguridad y uso de estándares y catálogos de la información de los registros electrónicos en salud[168] y por otra parte, las recomendaciones al proyecto de implementación del Servicio Nacional de

[165] Real, A. (Coord.). (2010). *Códigos de Conducta y actividad económica: una perspectiva jurídica*. Madrid: Editorial Marcial Pons.

[166] Disponible en: http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf.

[167] Su denominación primero cambió a Instituto Federal de Acceso a la Información y Protección de Datos en virtud del artículo transitorio sexto de la LFPDPPP y posteriormente su nombre actual en virtud de la Ley General de Transparencia y Acceso a la Información Pública. Esta última fue publicada en el *Diario Oficial de la Federación* de 4 de mayo de 2015. Disponible en: http://inicio.ifai.org.mx/MarcoNormativoDocumentos/Decreto%20-%20Ley%20General%20de%20Transparencia.pdf.

[168] Disponible en: http://inicio.ifai.org.mx/RecomendacionesRecientes/RECOMENDACIONES_%20AL_%20ANTEPROYECTO_%20DE_%20NOM-024-SSA3-2007.pdf.

Identificación Personal (SNIP) y eventual expedición de la Cédula de Identidad Ciudadana y Personal.[169]

Ambos casos, aunque se trate de expedientes relativos a la verificación del cumplimiento de la protección de datos personales de cada uno de los proyectos, son ejemplos del resultado de la evaluación de impacto en la protección de datos personales, como proceso que tiene por objeto evaluar los riesgos que el tratamiento de los datos personales puede implicar para los titulares y que permite, en su caso, adoptar medidas técnicas y organizativas para mitigarlos.

En los antecedentes de las recomendaciones al proyecto de implementación de la cédula de identidad se indica que es necesario contar con un proyecto que "garantice el derecho fundamental a la protección de los datos personales consagrado en el segundo párrafo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos" por lo que el INAI "inició los primeros acercamientos con la Secretaría de Gobernación con el propósito de verificar el cumplimiento de la normatividad vigente aplicable a la materia y acompañar a dicha dependencia en la implementación de un proyecto que garantice la protección de los datos personales desde su inicio" y para ello una PIA (*Privacy Impact Assessment* por sus siglas) que se concretó en el análisis del Acuerdo Técnico del proyecto de implementación del SNIP y expedición de la cédula de identidad.

## III. Análisis del contenido

**1. Esquemas de mejores prácticas en protección de datos personales.** En relación con los esquemas de mejores prácticas en protección de datos personales, debe atenderse a la mención incluida en el Dictamen de las Comisiones Unidas de Gobernación y de Estudios Legislativos Primera, que indica que el objeto de éstos es:

I. Elevar el nivel de protección de datos personales.

II. Armonizar el tratamiento de datos personales en un sector específico.

III. Facilitar el ejercicio de los derechos de acceso, rectificación, cancelación u oposición por parte de los titulares.

IV. Complementar las disposiciones previstas en la normatividad que resulte aplicable en materia de protección de datos personales, y

V. Demostrar ante el Instituto o, en su caso, los organismos garantes, el cumplimiento de la normatividad que resulte aplicable en materia de protección de datos personales.[170]

[169] Disponible en: http://inicio.ifai.org.mx/RecomendacionesRecientes/Recomendacion_SNIP-CEDI-28abril10.pdf.

[170] Senado de la República. (2016). *Dictamen de las Comisiones Unidas de Gobernación y de Estudios Legislativos Primera, con Proyecto de Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, p. 72.

El Dictamen también indica que en el texto de la propuesta se desarrolla “la validación o reconocimiento de los esquemas de mejores prácticas”, lo que finalmente se incorporó al articulado de la LGPDPPSO en los artículos 72 y 73 que se comentan a continuación.

En concreto, el artículo 72 de la LGPDPPSO está dedicado al objeto de los esquemas de mejores prácticas en protección de datos personales, destacando que son un instrumento “para el cumplimiento de las obligaciones” previstas en la LGPDPPSO.

Con respecto a la versión objeto del Dictamen de las Comisiones Unidas de Gobernación y de Estudios Legislativos Primera, la LGPDPPSO incluye, en la fracción IV, recorriendo las subsiguientes, que dichos esquemas podrán tener también por objeto “facilitar las transferencias de datos personales”.

La validación o reconocimiento de los esquemas de mejores prácticas en protección de datos personales por el INAI o, en su caso, los organismos garantes, es objeto del artículo 73 de la LGPDPPSO.

Para que el esquema pueda ser validado o reconocido por el INAI o, en su caso, los organismos garantes, será necesario que se cumplan dos requisitos acumulativos que son, por una parte, que se cumpla con los parámetros que emitan el INAI o los organismos garantes conforme a los requisitos que fije el primero y, por otra parte, que sean notificados al INAI o al organismo garante correspondiente siguiendo el procedimiento que se establece en los citados parámetros. La notificación permitirá que los esquemas “sean evaluados y, en su caso, validados o reconocidos e inscritos en el registro” que será administrado por el INAI en virtud de la función que le atribuye la fracción XV del artículo 89 de la LGPDPPSO.

No obstante, tanto el INAI como los organismos garantes, según corresponda, emitirán las reglas de operación aplicables a sus respectivos registros para la inscripción de los esquemas de mejores prácticas en protección de datos personales validados o reconocidos y podrán ser inscritos en el registro administrado por el INAI.

Lo anterior debe interpretarse a la vista de la fracción XVIII del artículo 89 de la LGPDPPSO, que indica que corresponde al INAI

> ... realizar las evaluaciones correspondientes a los esquemas de mejores prácticas que les sean notificados, a fin de resolver sobre la procedencia de su reconocimiento o validación e inscripción en el registro de esquemas de mejores prácticas, así como promover la adopción de los mismos.

Sobre esta materia, cabría considerar la experiencia adquirida por el INAI en el caso del sector privado, ya que en virtud de la normatividad aplicable se emitieron los Parámetros de Autorregulación en materia de Protección de Datos Personales[171] y se creó el Registro de Esquemas de Autorregulación Vinculante (REA)[172] cuyo funcionamiento queda sujeto a las Reglas de Operación del Registro de Esquemas de Autorregulación Vinculante.[173]

**2. Tratamiento intensivo o relevante de datos personales.** El concepto relativo al tratamiento intensivo o relevante de datos personales no se define en el artículo 3 de la LGPDPPSO, ni en el artículo 75 de la misma, aunque este último incluye los criterios a considerar si se está ante dichos tratamientos de datos personales.

Los tres factores para evaluar si el tratamiento de los datos personales es intensivo o relevante son los siguientes: 1) existen riesgos inherentes a los datos personales a tratar (fracción I), 2) los datos personales objeto de tratamiento son sensibles (fracción II) y 3) se efectúan o pretenden efectuar transferencias de datos (fracción III).

Si existen riesgos inherentes a los datos personales a tratar, es necesario considerar si esos riesgos son iguales a los que se presentan en el sector privado por lo que se refiere en el artículo 60 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, al "riesgo inherente por tipo de dato personal" como factor para determinar las medidas de seguridad que deberán establecer y mantener los responsables y encargados del tratamiento.

No obstante, si bien se trata de un factor relevante, en última instancia se debe considerar el riesgo que implique el tratamiento de datos personales para su titular. Es decir, se busca proteger a la persona, titular de los datos personales, lo que implica atender al riesgo que conlleva o puede implicar el tratamiento de sus datos personales, siendo la sensibilidad de los datos personales uno de los criterios aplicables, tal como hace la normatividad en México, tanto en el sector privado como en el público.

Lo anterior da lugar a que el segundo de los factores que se presentan sea, precisamente, la sensibilidad de los datos personales objeto de tratamiento, debiendo atender en este caso a la definición de datos personales sensibles que, conforme a la fracción X del artículo 3 de la LGPDPPSO, son:

---

[171] Publicados en el *Diario Oficial de la Federación* el 29 de mayo de 2014. Estos Parámetros abrogaron los Parámetros para el correcto desarrollo de los esquemas de autorregulación vinculante a que se refiere el artículo 44 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación,* 17 de enero de 2013.

[172] Para más información sobre el REA puede verse http://rea.inai.org.mx/

[173] Acuerdo del Pleno del Instituto Federal de Acceso a la Información y Protección de Datos por el que se aprueba el Proyecto de Reglas de Operación del Registro de Esquemas de Autorregulación Vinculante y se instruye su publicación oficial, *Diario Oficial de la Federación,* 18 de febrero de 2015.

Sobre los Esquemas de Autorregulación Vinculante en la LFPDPPP véase Reyes, A. (2013). "La legislación mexicana en materia de protección de datos personales: autorregulación y sellos de confianza", en Ornelas, L. y Piñar, J. (Coords.), *La Protección de Datos Personales en México*. México: Tirant Lo Blanch, p. 379 y ss.

> 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 mas 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.

Esta definición sigue, en gran medida, la proporcionada por la fracción VI del artículo 3 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (sobre el tratamiento de los datos de salud como un supuesto de datos sensibles).[174]

El tercer factor es relativo a efectuar o pretender efectuar transferencias internacionales de datos, que pueden ser tanto nacionales como internacionales. Al respecto, en cualquier caso, dichas transferencias se producirán entre dos o más responsables del tratamiento. Es decir, la transferencia implica, según la definición de la misma en la fracción XXXII del artículo 3 de la LGPDPPSO, que se trata de "toda comunicación de datos personales dentro o fuera del territorio mexicano, realizada a persona distinta del titular, del responsable o del encargado", por lo que es aquella en virtud de la que un responsable del tratamiento transfiere o comunica a otro u otros responsables del tratamiento los datos personales, ya se encuentre este último en territorio mexicano o fuera del mismo.

Sin perjuicio de lo anterior, hay que mencionar que una de las funciones que se atribuyen al Sistema Nacional, en virtud de la fracción XIX del artículo 14 de la LGPDPPSO, es la relativa a expedir criterios adicionales para determinar los supuestos en los que se está ante un tratamiento intensivo o relevante de datos personales, refiriéndose expresamente a los artículos 70 y 71 de la LGPDPPSO. Por tanto, dichos criterios adicionales podrían servir para aclarar cuándo un tratamiento de datos personales es intensivo o relevante.

Esta función es objeto del artículo 76 de la LGPDPPSO, el cual indica que el Sistema Nacional "podrá emitir criterios adicionales con sustento en parámetros objetivos que determinen que se está en presencia de un tratamiento intensivo o relevante de datos personales".

Estos criterios serán emitidos de conformidad con lo previsto en el comentado artículo 75 de la LGPDPPSO y en función de los factores que se establecen en el artículo 76 de la misma, que son los siguientes: "I. El número de titulares; II. El público objetivo; III. El desarrollo de la tecnología utilizada, y IV. La relevancia del tratamiento de datos personales en atención al impacto social o, económico del mismo, o bien, del interés público que se persigue".

[174] Canales, Á. (2013). "La protección de datos en el sector sanitario", en Ornelas, L. y Piñar, J.(Coords), *La Protección de Datos Personales en México.* México: Tirant Lo Blanch, p. 429 y ss.

Dichos factores deben entenderse como una lista exhaustiva o *numerus clausus* al no contemplarse ninguna cláusula adicional al respecto.

Por último, como se indicaba en el Informe de gestión 2015-2016 de la Comisión de Protección de Datos Personales, tanto estos criterios como las disposiciones administrativas para la valoración del contenido de las evaluaciones de impacto en la protección de datos personales "están a reserva de lo que las y los integrantes de la Comisión de Protección de Datos Personales identifiquen".[175]

**3. Evaluación de impacto en la protección de datos personales.** La LGPDPPSO, en la fracción XVI del artículo 3, define el concepto de evaluación de impacto en la protección de datos personales de la siguiente manera:

> Documento mediante el cual los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales, valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable.

La definición permite adelantar algunas cuestiones relevantes en relación con la elaboración de evaluaciones de impacto en la protección de datos personales que posteriormente son objeto de los artículos 74 a 79 de la LGPDPPSO.

En particular, las cuestiones que derivan de la mencionada definición son que dicha evaluación de impacto en la protección de datos personales se materializa a través de un documento elaborado por los sujetos obligados (el responsable y el encargado del tratamiento) para identificar y mitigar posibles riesgos para el titular de los datos personales relacionados con el cumplimiento de la normativa aplicable en materia de protección de datos personales, cuando se produzca un tratamiento intensivo o relevante de datos personales en los casos indicados en la definición.

En cuanto al desarrollo de este concepto en el articulado de la LGPDPPSO, el primer párrafo del artículo 74 repite en buena medida la definición previamente dada en el ya citado artículo 3, si bien a diferencia de

[175] Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2016). *Informe de Gestión 2015-2016 de la Comisión de Protección de Datos Personales*, p. 50. [Archivo PDF]. Disponible en: http://snt.org.mx/images/Doctos/Informe_de_Geston_2015_2016_CPDP_SNT-09-11-2016.pdf [fecha de consulta: 5 de mayo 2018].

aquél, menciona que es el responsable, entendiéndose como el responsable del tratamiento, omitiendo por tanto la referencia al encargado del tratamiento, quien tendrá que realizar una evaluación de impacto en la protección de datos cuando "pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio y de conformidad con esta Ley impliquen el tratamiento intensivo o relevante de datos personales".

Es decir, tienen que concurrir dos requisitos para que el responsable tenga que realizar una evaluación de impacto relativa a la protección de datos, los cuales son: 1) que pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología y 2) que a su juicio y considerando, tanto lo dispuesto en la LGPDPPSO como, en su caso, los criterios adicionales que pudiera emitir el Sistema Nacional de Transparencia, impliquen el tratamiento intensivo o relevante de datos personales.

Si se atiende al citado Dictamen de las Comisiones Unidas de Gobernación y de Estudios Legislativos Primera, cabe poner de manifiesto que en la LGPDPPSO no se ha incluido el supuesto relativo a elaborar anteproyectos de leyes, decretos o actos administrativos de carácter general relacionados con el tratamiento de datos personales, lo que significa que no habrá ninguna obligación de realizar dicha evaluación en estos casos.

Además, como indica el artículo 77 de la LGPDPPSO, los sujetos obligados que realicen una evaluación de impacto en la protección de datos personales tienen que cumplir con la obligación de presentarla, según corresponda, al INAI o al organismo garante correspondiente para que, en su caso, emitan sus recomendaciones no vinculantes.

El plazo para que los sujetos obligados presenten su evaluación de impacto en la protección de datos personales es de treinta días anteriores a la fecha en que se pretende poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología. El INAI y los organismos garantes, según corresponda, tendrán que emitir sus recomendaciones no vinculantes en el plazo de "treinta días siguientes contados a partir del día siguiente a la presentación" según indica el párrafo segundo del artículo 78 de la LGPDPPSO.

Cabe destacar el importante papel previsto en los artículos objeto de comentario del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales ya que, en virtud del último párrafo del artículo 74 de la LGPDPPSO, tendrá que determinar el contenido de la evaluación de impacto en la protección de datos personales y en virtud del

artículo 76 de la LGPDPPSO "podrá emitir criterios adicionales con sustento en parámetros objetivos que determinen que se está en presencia de un tratamiento intensivo o relevante de datos personales".

No obstante, el artículo 79 de la LGPDPPSO incluye una importante excepción a la obligación de los sujetos obligados de realizar una evaluación de impacto en la protección de datos personales. De modo que los sujetos obligados no tendrán que realizarla cuando: 1) a juicio del sujeto obligado se puedan comprometer los efectos que se pretende lograr con la posible puesta en operación o modificación de políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento intensivo o relevante de datos personales o 2) se trate de una situación de emergencia o urgencia.

Este último artículo no dice si el sujeto tendrá que justificar, documentándolo de alguna manera, cualquiera de estas situaciones o adoptar cualesquiera otras medidas para mitigar el riesgo que implique el tratamiento de datos personales.

Por último, la LGPDPPSO tampoco prevé que no realizar o presentar la evaluación de impacto en la protección de datos personales por los sujetos obligados suponga una infracción a la LGPDPPSO que pudiera dar lugar a amonestación pública o multas. No obstante, que sea una mejor práctica puede explicar que el no realizarla no conlleve sanción.

**4. Algunas consideraciones adicionales.** El análisis del articulado relativo a las mejores prácticas en materia de protección de datos personales da lugar a que puedan plantearse algunas cuestiones específicas, tanto por lo que se refiere a los esquemas de mejores prácticas en la materia como al concepto de tratamiento intensivo o relevante de datos personales y a la evaluación de impacto en la protección de datos personales.

En el caso de los esquemas de mejores prácticas en materia de protección de datos es importante señalar que al momento de emitir los correspondientes parámetros se preste especial atención a que los responsables adopten e implementen dichos esquemas para, en particular, cumplir con altos estándares en materia de protección de datos personales que, incluso, superen los previstos en la normativa con la que tienen que cumplir y que puedan considerar instrumentos adecuados a tal fin, ya sean códigos tipo o de conducta, sellos o certificaciones y que dichos parámetros puedan adecuarse conforme avancen, tanto a escala nacional como internacional, las mejores prácticas en materia de protección de datos personales.

De esta manera, México se alinearía con altos estándares internacionales y la práctica seguida en la materia a escala internacional, ya que, por ejemplo,

en el caso del Reglamento General de Protección de Datos[176] de la Unión Europea los códigos de conducta adquieren una relevancia trascendental, ya que por medio de los mismos "se especifican o traducen a un sector dado las obligaciones de responsables y encargados —obligaciones que varían según el riesgo para los derechos y libertades de la persona— y para que ese código sea aprobado debe aportar un valor añadido en términos de claridad porque aborde adecuadamente la problemática específica del tratamiento en un sector concreto y porque aporte soluciones".[177]

Por lo que se refiere al concepto de tratamiento intensivo o relevante de datos personales, los criterios que se emitan al respecto aportarán claridad y facilitarán la implementación de la normativa en materia de protección de datos, debiendo considerar en particular, el tratamiento analítico de los datos personales y el riesgo que, en su caso, implique el tratamiento de datos personales sensibles para la persona a la que se refieren los mismos. Es así que, sin perjuicio de los factores incluidos en la LGPDPPSO, el tratamiento intensivo o relevante requiere considerar, en particular, el riesgo que el mismo pudiera representar para el titular de los datos personales.

En cuanto a la evaluación de impacto en la protección de datos personales, debe ponerse especial atención a que el riesgo afecte a la persona física a la que se refieren los datos personales objeto de tratamiento. Al respecto, deben considerarse también los criterios emitidos por otras autoridades de protección de datos personales en el ámbito internacional como, por ejemplo, las Directrices sobre la Evaluación de Impacto en la Protección de Datos que emitió el Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE para proporcionar una guía sobre dicho concepto en el Reglamento general de protección de datos.[178]

## IV. Conclusiones

Las mejores prácticas en materia de protección de datos personales, entendidas como acciones preventivas, como los esquemas o la evaluación de impacto en la protección de datos personales, deben ser promovidas y fomentadas dado que facilitarán, por una parte, elevar el nivel de protección de datos personales, superando así, incluso, el nivel de cumplimiento previsto en

[176] 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), *Diario Oficial de la Unión Europea*, L 119, el 4 de mayo de 2016.

[177] Díaz-Romeral, A. (2016). "Los códigos de conducta en el Reglamento General de Protección de Datos" en Piñar, J. (Dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*. Madrid, España: Editorial Reus, p. 389.

[178] Grupo de Trabajo del Artículo 29. (2017). *Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento entraña probablemente un alto riesgo a efectos del Reglamento (UE) 2016/679, WP 248*. Adoptadas el 4 de abril. Revisadas por última vez y adoptadas el 4 de octubre de 2017.

la normativa aplicable y, por otra parte, crear, al mismo tiempo, una cultura de protección de datos personales.

También es importante que México considere implementar altos estándares internacionales en materia de protección de datos personales para alinearse con el resto del mundo en relación con las buenas prácticas en esta materia.

Finalmente, es necesario que el Sistema Nacional de Transparencia, a través de los correspondientes criterios y parámetros, desarrolle las previsiones de algunos de los artículos comentados. Dichos criterios y parámetros serán también una oportunidad para que todas las partes involucradas colaboren para que las mejores prácticas permitan a los sujetos obligados cumplir y ser responsables en virtud del principio de responsabilidad (en inglés, *accountability*).[179]

## Referencias

Acuña, F. (2016). "La protección de datos personales y notas sobre los desafíos de Internet" en Recio, M. (Coord.), *La Constitución en la sociedad y economía digitales: Temas selectos de derecho digital mexicano*. México: Centro de Estudios Constitucionales, Suprema Corte de Justicia de la Nación.

Canales, Á. (2013). "La protección de datos en el sector sanitario", en Ornelas, L. y Piñar, J. (Coords), *La Protección de Datos Personales en México*. México: Tirant Lo Blanch.

Díaz-Romeral, A. (2016). "Los códigos de conducta en el Reglamento General de Protección de Datos" en Piñar, J. (Dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*. Madrid, España: Editorial Reus.

Piñar, J. y Ornelas, L. (Coords.). (2013). *La Protección de Datos Personales en México*. México: Tirant Lo Blanch.

Piñar, J. (2015). "Normalizar la cultura de la protección de datos", en la obra colectiva *Veinte años de protección de datos en España*. Madrid, España: Agencia Española de Protección de Datos.

Real, A. (Coord.). (2010). *Códigos de Conducta y actividad económica: una perspectiva jurídica*. Madrid, España: Editorial Marcial Pons.

[179] El principio de responsabilidad se recoge en el artículo 14 de la LFPDPPP y en el artículo 29 de la LGPDPPSO.

Reyes, A. (2013). “La legislación mexicana en materia de protección de datos personales: autorregulación y sellos de confianza”, en Ornelas, L. y Piñar, J. (Coords.), *La Protección de Datos Personales en México*. México: Tirant Lo Blanch, Monografías.

Senado de la República. (2015). *Dictamen de las Comisiones Unidas de Gobernación y de Estudios Legislativos Primera, con Proyecto de Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados*. [Archivo PDF]. Disponible en: http://www.senado.gob.mx/comisiones/gobernacion/docs/proteccion_datos/Documento3.pdf, [fecha de consulta: 3 de mayo 2018].

Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2016). *Informe de Gestión 2015-2016 de la Comisión de Protección de Datos Personales*, p. 50. [Archivo PDF]. Disponible en: http://snt.org.mx/images/Doctos/Informe_de_Geston_2015_2016_CPDP_SNT-09-11-2016.pdf [fecha de consulta: 5 de mayo 2018].

# CAPÍTULO II
# DE LAS BASES DE DATOS EN POSESIÓN DE INSTANCIAS DE SEGURIDAD, PROCURACIÓN Y ADMINISTRACIÓN DE JUSTICIA

***Artículo 80.*** *La obtención y tratamiento de datos personales, en términos de lo que dispone esta Ley, por parte de las sujetos obligados competentes en instancias de seguridad, procuración y administración de justicia, está limitada a aquellos supuestos y categorías de datos que resulten necesarios y proporcionales para el ejercicio de las funciones en materia de seguridad nacional, seguridad pública, o para la prevención o persecución de los delitos. Deberán ser almacenados en las bases de datos establecidas para tal efecto.*

*Las autoridades que accedan y almacenen los datos personales que se recaben por los particulares en cumplimiento de las disposiciones legales correspondientes, deberán cumplir con las disposiciones señaladas en el presente Capítulo.*

***Artículo 81.*** *En el tratamiento de datos personales así como en el uso de las bases de datos para su almacenamiento, que realicen los sujetos obligados competentes de las instancias de seguridad, procuración y administración de justicia deberá cumplir con los principios establecidos en el Título Segundo de la presente Ley.*

*Las comunicaciones privadas son inviolables. Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada.*

***Artículo 82.*** *Los responsables de las bases de datos a que se refiere este Capítulo, deberán establecer medidas de seguridad de nivel alto, para garantizar la integridad, disponibilidad y confidencialidad de la información,*

*que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.*

## COMENTARIO

**Mónica Estrada Tanck**

### I. Antecedentes

El presente capítulo tiene por objeto plantear el tema de la entrega de información relativa a datos personales por parte de empresas privadas a las autoridades encargadas de atribuciones de seguridad y justicia como parte de la colaboración necesaria que existe, para ciertos casos, entre el sector privado y el público, para el debido desempeño de las atribuciones de las mencionadas autoridades.

Si bien es cierto que existen diversos ordenamientos jurídicos que regulan la citada colaboración,[180] es importante señalar que el capítulo relativo a las bases de datos en posesión de instancias de seguridad, procuración y administración de justicia, contenido en la LGPDPPSO, tiene como antecedente inmediato el tema de colaboración con la justicia por parte de concesionarios y autorizados en materia de telecomunicaciones, por lo que respecta a la información sobre geolocalización y otros datos relativos a comunicaciones privadas.[181]

A este respecto, el 11 de junio de 2013 se publicó en el DOF[182] la reforma en materia de telecomunicaciones en México. Posteriormente se emitió la nueva Ley Federal de Telecomunicaciones y Radiodifusión,[183] la cual, en su capítulo De las Obligaciones en materia de Seguridad y Justicia del Título Octavo De la Colaboración con la Justicia, artículos 189 y 190, fracciones I a IV y último párrafo establece lo siguiente:

---

[180] Cfr. Artículos 291 y 303 del Código Nacional de Procedimientos Penales, *Diario Oficial de la Federación,* 5 de marzo de 2014. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_170616.pdf
Véase otras leyes en Red en Defensa de los Derechos Digitales (R3D). (2016). *El Estado de la Vigilancia, Fuera de Control*. México: R3D, p. 17. [Archivo PDF]. Disponible en: https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016-FINAL1.pdf, [fecha de consulta: 5 de mayo 2018].

[181] Cámara de Diputados. (2016). *Dictamen que emite la Comisión de Transparencia y Anticorrupción de la Cámara de Diputados con relación a la Minuta con Proyecto de Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, pp. 38 a 40, 65, 66, 75, 81, 82, 90 y 91. [Archivo PDF]. Disponible en: https://sontusdatos.org/wp-content/uploads/2016/11/Dictamen-LGPDP-en-t%C3%A9rminos-de-la-Minuta-Datos-Personales-2.pdf, [fecha de consulta: 5 de mayo 2018].Cabe señalar que la Cámara de Diputados aprobó sin cambios la Minuta enviada por el Senado.

[182] Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5301941&fecha=11/06/2013

[183] Ley Federal de Telecomunicaciones y Radiodifusión, *Diario Oficial de la Federación,* 14 de julio de 2014. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5352323&fecha=14/07/2014

**Artículo 189. Los concesionarios de telecomunicaciones y, en su caso, los autorizados y proveedores de servicios de aplicaciones y contenidos están obligados a atender todo mandamiento por escrito, fundado y motivado de la autoridad competente en los términos que establezcan las leyes.**

Los titulares de las instancias de seguridad y procuración de justicia designarán a los servidores públicos encargados de gestionar los requerimientos que se realicen a los concesionarios y recibir la información correspondiente, mediante acuerdos publicados en el Diario Oficial de la Federación.

**Artículo 190.** Los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán:

**I. Colaborar con las instancias de seguridad, procuración y administración de justicia, en la localización geográfica, en tiempo real, de los equipos de comunicación móvil, en los términos que establezcan las leyes.**

Cualquier omisión o desacato a estas disposiciones será sancionada por la autoridad, en los términos de lo previsto por la legislación penal aplicable.

**El Instituto, escuchando a las autoridades a que se refiere el artículo 189 de esta Ley, establecerá los lineamientos que los concesionarios de telecomunicaciones y, en su caso, los autorizados deberán adoptar para que la colaboración a que se refiere esta Ley con dichas autoridades, sea efectiva y oportuna;**

**II. Conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los siguientes datos:**

a) Nombre, denominación o razón social y domicilio del suscriptor;

b) Tipo de comunicación (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluidos el reenvío o transferencia de llamada) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia y avanzados);

c) Datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago;

d) Datos necesarios para determinar la fecha, hora y duración de la comunicación, así como el servicio de mensajería o multimedia;

e) Además de los datos anteriores, se deberá conservar la fecha y hora de la primera activación del servicio y la etiqueta de localización (identificador de celda) desde la que se haya activado el servicio;

f) En su caso, identificación y características técnicas de los dispositivos, incluyendo, entre otros, los códigos internacionales de identidad de fabricación del equipo y del suscriptor;

g) La ubicación digital del posicionamiento geográfico de las líneas telefónicas, y

h) La obligación de conservación de datos, comenzará a contarse a partir de la fecha en que se haya producido la comunicación.

Para tales efectos, **el concesionario deberá conservar los datos referidos en el párrafo anterior durante los primeros doce meses en sistemas que permitan su consulta y entrega en tiempo real a las autoridades competentes, a través de medios electrónicos. Concluido el plazo referido, el concesionario deberá conservar dichos datos por doce meses adicionales en sistemas de almacenamiento electrónico**, en cuyo caso, la entrega de la información a las autoridades competentes se realizará dentro de las cuarenta y ocho horas siguientes, contadas a partir de la notificación de la solicitud.

[…]

**Los concesionarios de telecomunicaciones y, en su caso, los autorizados, tomarán las medidas técnicas necesarias respecto de los datos objeto de conservación, que garanticen su conservación, cuidado, protección, no manipulación o acceso ilícito, destrucción, alteración o cancelación, así como el personal autorizado para su manejo y control.**

**Sin perjuicio de lo establecido en esta Ley, respecto a la protección, tratamiento y control de los datos personales en posesión de los concesionarios o de los autorizados, será aplicable lo dispuesto en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares;**

**III. Entregar los datos conservados a las autoridades a que se refiere el artículo 189 de esta Ley, que así lo requieran, conforme a sus atribuciones, de conformidad con las leyes aplicables.**

> **Queda prohibida la utilización de los datos conservados para fines distintos a los previstos en este capítulo, cualquier uso distinto será sancionado por las autoridades competentes en términos administrativos y penales que resulten.**
>
> Los concesionarios de telecomunicaciones y, en su caso, los autorizados, están obligados a entregar la información dentro de un plazo máximo de veinticuatro horas siguientes, contado a partir de la notificación, siempre y cuando no exista otra disposición expresa de autoridad competente;
>
> […]
>
> **Las comunicaciones privadas son inviolables. Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada.**[184]

Una vez expedida la mencionada ley, se generó una discusión pública importante en relación con el posible exceso en las disposiciones citadas, específicamente en lo que se refiere a si existe o no la necesidad de una autorización judicial para los requerimientos de información o si solamente es necesaria para algunos casos (donde se excluyen, por ejemplo, los requerimientos de información sobre geolocalización en tiempo real por no considerarlo comunicación privada en términos del artículo 16 constitucional); autoridades facultadas para realizar los requerimientos; exceso en los plazos de conservación de la información; falta de precisión en cuanto a las motivaciones que pueden tener los requerimientos de información por parte de la autoridad (lo cual permitiría demasiada generalidad en los mencionados requerimientos); falta de regulación en temas como notificación diferida a la persona investigada, retención masiva de datos,[185] etc.

---

[184] Texto resaltado por la autora.

[185] En relación con la retención masiva de datos, como referencia puede citarse que el Tribunal de Justicia de la Unión Europea y el Relator Especial de la ONU sobre el derecho a la libertad de expresión, han advertido la incompatibilidad de normas de retención masiva de datos con el derecho a la privacidad, y que no está comprobado que la retención de datos (incluso después de terminada la relación empresa-cliente) efectivamente tenga impacto en la persecución de delitos graves. Al respecto véanse el comunicado de prensa de la sentencia del TJUE en los asuntos acumulados C-293/12 y C-594/12 Digital Rights Ireland y Seitlinger y otros. Disponible en: https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054es.pdf, así como el "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", A/HRC/23/40. Disponible en: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf. Este último documento señala en su párrafo 67: "Las leyes de retención de datos son invasivas y costosas, y amenazan los derechos de privacidad y libertad de expresión. El hecho de obligar a proveedores de servicios de comunicaciones a crear enormes bases de datos con información sobre quién se comunica con quién a través del teléfono o el Internet, la duración de la comunicación, así como la ubicación del usuario, y el hecho de resguardar dicha información (en ocasiones por años), hace que las leyes de retención de datos incrementen de manera importante el ámbito de vigilancia estatal, y por tanto la amplitud de violaciones a derechos humanos. Las bases de datos con este tipo de información se vuelven vulnerables al robo, fraude y difusión accidental". (Traducción propia).

Ahora bien, todos los datos que se recaban, en virtud de estas normas, incluso aquellos referidos a la geolocalización, deben considerarse datos personales por referirse a personas físicas identificadas o identificables. Así, la Ley Federal de Telecomunicaciones y Radiodifusión sí estableció ciertos parámetros que deben seguir los concesionarios y autorizados en el resguardo y transferencia de los datos personales, señalando que deberán adoptar las medidas técnicas necesarias respecto de los datos objeto de conservación, que garanticen su conservación, cuidado, protección, no manipulación o acceso ilícito, destrucción, alteración o cancelación, así como el personal autorizado para su manejo y control, con la remisión correspondiente a la ley aplicable a dichos concesionarios y autorizados, esto es, la LFPDPPP. Asimismo, se incluye una alusión al principio de finalidad en el segundo párrafo de la fracción III del artículo 190.

No obstante, lo cierto es que dicha ley no hace referencia a disposiciones específicas aplicables a las autoridades que recabarían estos datos. Hasta el momento de la expedición de la ley (julio de 2014), a las autoridades federales, como sujetos obligados en materia de protección de datos personales, les eran aplicables las disposiciones genéricas en materia de protección de datos personales contenidas en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.[186]

Por otra parte, con fundamento en el último párrafo de la fracción I del artículo 190 de la Ley Federal de Telecomunicaciones y Radiodifusión, el Instituto Federal de Telecomunicaciones expidió los Lineamientos de Colaboración en materia de Seguridad y Justicia,[187] los cuales señalan, entre otras cosas, lo siguiente:

> **OCTAVO.** La o las Plataformas Electrónicas que los Concesionarios y Autorizados deberán utilizar para dar cumplimiento a los requerimientos electrónicos de localización geográfica en tiempo real de los equipos de comunicación móvil, así como de entrega de datos conservados por los Concesionarios y Autorizados, deberán contar con las siguientes características:

[186] Dichas disposiciones seguirían siendo aplicables aún después de expedidas las leyes General y Federal de Transparencia y Acceso a la Información Pública, toda vez que dichas leyes, si bien establecieron algunas normas generales en materia de protección de datos, en sus disposiciones transitorias, señalaron que hasta en tanto no se expidiera la Ley General de Protección de Datos Personales para Sujetos Obligados, las disposiciones vigentes en la materia seguirían siendo aplicables.

[187] Instituto Federal de Telecomunicaciones. Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones expide los Lineamientos de Colaboración en materia de Seguridad y Justicia y modifica el Plan Técnico fundamental de numeración, publicado el 21 de junio de 1996, *Diario Oficial de la Federación,* 2 de diciembre de 2015. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5418339&fecha=02/12/2015

[…]

VII. **El Instituto solicitará periódicamente a los titulares de las Autoridades Facultadas la información relativa a las medidas implementadas o a implementarse para asegurar que el resguardo y manejo de la información de localización geográfica y de registro de datos recibida se realice mediante el uso de protocolos de seguridad de la información y/o herramientas digitales tales como herramientas de Cifrado, firmas o sellos digitales. De la misma manera, el Instituto solicitará a los titulares de las Autoridades Facultadas los protocolos utilizados para la cancelación o supresión segura de la información recibida, una vez cumplido el fin para el cual fue solicitada.** Dichos protocolos podrán tomar como base estándares internacionales, tales como: ISO/IEC 27001 Information technology Security techniques Information security management systems Requirements, NIST Special Publication 80053 Security and Privacy Controls for Federal Information Systems and Organizations y/o ETSI TS 102 656 Lawful Interception (LI); Retained Data; Requirements of Law Enforcement Agencies for handling Retained Data;

[…]

**DÉCIMO SEGUNDO. El registro de datos de comunicaciones materia de estas disposiciones se refiere a la conservación de los datos enlistados en la fracción II del artículo 190 de la LFTR. Las comunicaciones privadas son inviolables. Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada.**

**DÉCIMO OCTAVO. Los Concesionarios y Autorizados deberán entregar al Instituto, en el mes de enero y julio de cada año, un informe semestral electrónico a través del mecanismo que para tales efectos establezca el Instituto, relativo al cumplimiento de los presentes Lineamientos.**

**Dicho informe deberá contener y observar lo siguiente:**

**I. El número total y por Autoridad Facultada, de requerimientos de información de localización geográfica en tiempo real y de registro de datos de comunicaciones, desglosando las recibidas, entregadas y no entregadas mensualmente**, utilizando el formato que se anexa a los presentes Lineamientos como Anexo II.

> II. En el mes de julio, deberán integrar, además, el informe referido en el lineamiento OCTAVO, fracción VI. III. En el mes de enero, deberán integrar, además, el informe referido en el lineamiento CUADRAGÉSIMO.
>
> **El Instituto solicitará a las Autoridades Designadas y/o Facultadas en el mes de enero y julio de cada año, un informe semestral relativo al número de requerimientos de localización geográfica en tiempo real y de registro de datos realizados, así como el número de registros de datos de comunicaciones cancelados y suprimidos de manera segura, una vez cumplido el fin para el cual fueron solicitados.**
>
> En términos de lo establecido en la Ley General de Transparencia y Acceso a la Información Pública y demás disposiciones aplicables, **las autoridades señaladas en los artículos 189 y 190 de la LFTR, están obligadas a adoptar las medidas necesarias que garanticen la seguridad de los Datos Personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.**
>
> La información estadística contenida en los informes semestrales será publicada en el portal de Internet del Instituto en términos de lo establecido en la Ley General de Transparencia y Acceso a la Información Pública y demás disposiciones aplicables.
>
> En términos de lo establecido en la Ley General de Transparencia y Acceso a la Información Pública y demás disposiciones aplicables, en caso de que los sistemas de conservación de datos hayan sido vulnerados y los Datos Personales de los usuarios finales se encuentren comprometidos, los Concesionarios y Autorizados deberán notificar inmediatamente a éstos e indicar las medidas que el usuario podrá tomar para disminuir o contrarrestar cualquier afectación derivada de esta vulneración.[188]

Como puede observarse, los citados Lineamientos sí contienen algunas disposiciones dirigidas a las autoridades que recaban los datos personales, específicamente en relación con medidas de seguridad para el resguardo y cancelación de los mismos.

Sin perjuicio del antecedente inmediato que hemos analizado, lo cierto es que existen otros cuerpos normativos que contienen disposiciones relativas a la entrega de datos personales en el marco de colaboración con instancias de seguridad y justicia, y que no únicamente se circunscriben al tema de telecomunicaciones. Asimismo, la normatividad citada se refiere únicamente a la materia federal —telecomunicaciones— y está dirigida, en su caso, a autoridades de esta naturaleza, por lo que pueden existir esquemas de colaboración con la justicia en el ámbito local.

[188] Texto resaltado por la autora.

## II. Relevancia temática y contexto

En virtud de lo señalado en el apartado anterior, durante la discusión de las iniciativas para expedir una ley general de protección de datos personales en posesión de sujetos obligados —a partir de la reforma constitucional del 7 de febrero de 2014— se advirtió que resultaba necesario contar con disposiciones jurídicas para cualquier tipo de entrega de información relativa a datos personales en el marco de la colaboración del sector privado con el sector público en temas de seguridad y justicia aplicable, tanto a autoridades federales como locales, a efecto de que dichas autoridades, los organismos garantes y (de manera muy relevante) los ciudadanos tengan claridad sobre los principios aplicables a dichos datos.

En efecto, durante las audiencias públicas, sostenidas en el Senado de la República, para la discusión de la mencionada iniciativa de ley general[189] se aportaron diversas ideas y propuestas para la inclusión de un capítulo sobre este tema, en especial por miembros de la sociedad civil y de la industria.

Entre los argumentos utilizados destaca que los gobiernos en ocasiones obtienen una gran cantidad de información invocando la seguridad nacional, cuestión que en ocasiones puede contraponerse con derechos individuales de privacidad. Por supuesto que los gobiernos deben tener la facultad de allegarse de este tipo de información, sin embargo, es importante establecer regulaciones que acoten estas atribuciones y determinen, de manera clara, que su ejercicio debe respetar los principios de protección de datos, en especial, el principio de licitud, también conocido en el derecho comparado como *the need to know basis* (necesidad de conocer) y el principio de la proporcionalidad.

En ese sentido, una ley de protección de datos para el sector público, claramente debía contener un apartado específico que abordara los requerimientos de instancias de seguridad, procuración y administración de justicia a empresas privadas en relación con información personal de sus clientes a efecto de dejar claro que deben cumplirse los principios de protección de datos, incluyendo, como se ha dicho, la proporcionalidad, necesidad de conocer (licitud), así como el derecho de los titulares de acceder a información

[189] Cámara de Diputados. (2016). *Dictamen que emite la Comisión de Transparencia y Anticorrupción de la Cámara de Diputados con relación a la Minuta con Proyecto de Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*. Cabe señalar que la Cámara de Diputados aprobó sin cambios la Minuta enviada por el Senado. En dicho Dictamen pueden consultarse los textos de las audiencias públicas del 1 de diciembre de 2015, 20 de enero y 5 de abril de 2016. En específico, las intervenciones de Carlos Brito (Red en Defensa de los Derechos Digitales) pp. 35 y 36; Lina Ornelas (Asociación Mexicana de Internet) pp. 38 a 40, 81 y 82; senadora Laura Angélica Rojas, pp. 65 y 66; Ana Cristina Ruelas (Artículo 19) p. 75; Ana Gaitán Uribe (Red en Defensa de los Derechos Digitales) pp. 78 y 79, y comisionado Oscar Guerra Ford (INAI) pp. 90 y 91. Disponibles en: https://sontusdatos.org/wp-content/uploads/2016/11/Dictamen-LGPDP-en-t%C3%A9rminos-de-la-Minuta-Datos-Personales-2.pdf

sobre dicha vigilancia estatal, una vez que la investigación no se encuentre en riesgo, y por último, medidas de seguridad adecuadas para el resguardo y transmisión. Analizaremos más adelante si estos extremos fueron incluidos en el capítulo correspondiente de la LGPDPPSO.

Asimismo, y como se ha mencionado, resultaba importante la inserción del capítulo correspondiente a la colaboración con instancias de seguridad y justicia por el hecho de que las autoridades federales y locales, así como los organismos garantes, requerían claridad sobre los principios aplicables a la entrega de este tipo de información —sea en el marco de las telecomunicaciones o no— pero además por una razón en extremo relevante: porque se trata de una excepción al principio de consentimiento, en virtud del cual, por ministerio de ley —y en la mayoría de los casos, a través de una orden judicial— un privado "distinto del titular y sin su conocimiento", entrega información sobre comunicaciones privadas de dicha persona. Más aún, dicha información se relaciona con investigaciones de naturaleza penal, por lo cual su transmisión se vuelve aún más relevante.

Ahora bien, después de la última audiencia pública en el Senado el 5 de abril de 2016, se insertó, en el dictamen que finalmente se aprobó en el Senado y en la Cámara de Diputados, el capítulo correspondiente en la LGPDPPSO.

Cabe señalar que la relevancia de este asunto ya había sido retomada en la Ley General de Transparencia y Acceso a la Información Pública[190] y en la Ley Federal[191] correspondiente, al establecer una obligación de transparencia para los sujetos obligados en materia de seguridad y justicia.

En efecto, el artículo 70, fracción XLVII de la Ley General de Transparencia y el artículo 69, fracción V inciso A de la Ley Federal de Transparencia establecen que deberá publicarse (y actualizarse cada tres meses) "para efectos estadísticos, el listado de solicitudes a las empresas concesionarias de telecomunicaciones y proveedores de servicios o aplicaciones de Internet para la intervención de comunicaciones privadas, el acceso al registro de comunicaciones y la localización geográfica en tiempo real de equipos

[190] Ley General de Transparencia y Acceso a la Información Pública, publicada en el *Diario Oficial de la Federación* el 4 de mayo de 2015. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP.pdf Véase Senado de la República. (2013). *Dictamen de las Comisiones Unidas de Anticorrupción y Participación Ciudadana, de Gobernación y de Estudios Legislativos, Segunda del Senado de la República; relativo a la iniciativa que contiene Proye cto de Decreto por el que se expide la Ley General de Transparencia y Acceso a la Información Pública*, específicamente las intervenciones de los senadores Zoé Robledo (p. 125) y Pilar Ortega (p. 126) y de la comisionada del Instituto Federal de Telecomunicaciones Adriana Labardini, p. 130. Disponible en: http://rendiciondecuentas.org.mx/wp-content/uploads/2015/03/Dictam-en-Transparencia-Aprobado-2013.03.18.pdf

[191] Ley Federal de Transparencia y Acceso a la Información Pública, publicada en el *Diario Oficial de la Federación* el 9 de mayo de 2016. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_270117.pdf

de comunicación, que contenga exclusivamente el objeto, el alcance temporal y los fundamentos legales del requerimiento, así como, en su caso, la mención de que cuenta con la autorización judicial correspondiente".

Esta obligación resulta relevante ya que la información correspondiente deberá estar disponible para el público en general en los sitios de internet de los sujetos obligados, sin necesidad de que el ciudadano efectúe solicitudes de acceso. Resultará interesante empatar esta información con los informes semestrales que deben presentar los sujetos obligados al Instituto Federal de Telecomunicaciones conforme al Cuadragésimo de los Lineamientos de Colaboración en materia de Seguridad y Justicia, citados anteriormente, con el número de requerimientos de localización geográfica en tiempo real y de registro de datos realizados, así como el número de registros de datos de comunicaciones cancelados y suprimidos de manera segura, una vez cumplido el fin para el cual fueron solicitados. Asimismo, otro elemento importante de información que deberá analizarse, serán los informes que las empresas requeridas deben presentar al Instituto Federal de Telecomunicaciones conforme al Lineamiento Décimo Octavo citado en el apartado anterior. Por último, pueden consultarse los Informes de Transparencia[192] que publican algunas empresas privadas en sus propios sitios para hacer del conocimiento público cuántos requerimientos de la autoridad han recibido en este tema.[193]

## III. Análisis del contenido

El artículo 16 de la CPEUM establece que será "la ley" la que regulará los derechos derivados de la garantía constitucional de protección de datos personales (acceso, rectificación, cancelación y oposición), los principios que rigen el tratamiento de dichos datos y "las excepciones a la aplicación de dichos principios".

A partir de la reforma de 2014 al artículo 6º constitucional en materia de transparencia y protección de datos resultaba claro que era la LGPDPPSO el asidero jurídico que debía detallar la regulación aplicable a cualquier excepción a los principios y derechos en materia de protección de datos —con independencia de que la excepción como tal pueda estar planteada en alguna otra ley o leyes, como hemos mencionado en apartados anteriores—. De esta manera se contiene en una sola ley la regulación relativa a los principios, derechos, deberes y excepciones aplicables al tratamiento de datos personales.

En ese sentido, por lo que se refiere a la excepción relativa a seguridad nacional y orden público, era necesario que la ley general detallara la manera en que los

[192] Véase: https://transparencyreport.google.com/, https://www.youtube.com/watch?v=MeKKHxcJfh0 y https://www.microsoft.com/en-us/about/corporate-responsibility/reports-hub.

[193] Cfr. Red en Defensa de los Derechos Digitales (R3D). (2016). *¿Quién defiende tus datos? 2016*. Disponible en: https://r3d.mx/wp-content/uploads/QDTD2016_v02_WEB.pdf y https://r3d.mx/2016/12/13/qdtd2016/, [fecha de consulta: 5 de mayo 2018].

sujetos obligados debían aplicar dicha excepción, proporcionando certeza jurídica tanto al ciudadano como a la autoridad sobre la manera en que debe aplicarse.

Así, la LGPDPPSO, en su artículo 80, señala que la obtención y tratamiento de datos personales por parte de los responsables competentes en el ámbito de seguridad, procuración y administración de justicia está limitada a aquellos supuestos y categorías de datos personales que resulten necesarios y proporcionales para el ejercicio de las funciones en materia de seguridad nacional y pública o para la prevención o persecución de los delitos.

Al respecto, en primer término habrá de irse acotando lo que se entiende por sujetos obligados competentes en instancias de seguridad, procuración y administración de justicia, remitiéndose a la normatividad que lo establezca,[194] ya que tendrá relación con el debido cumplimiento del principio de licitud. Cabe señalar que son las leyes en sentido formal y material —y no ordenamientos jurídicos de jerarquía inferior— las que deben establecer las autoridades que tienen facultades para solicitar este tipo de información, considerando que se trata de una excepción a los principios de protección de datos y que por tanto, resulta aplicable el artículo 16 constitucional antes citado.

Se señala que la obtención y tratamiento de los datos está limitada a aquellos supuestos y categorías de datos que resulten "necesarios y proporcionales" para el ejercicio de las funciones en materia de seguridad nacional y pública o para la prevención o persecución de los delitos. Ello implica que únicamente aquellos datos que se relacionen directamente con el cumplimiento de las atribuciones en materia de seguridad nacional, seguridad pública o prevención y persecución del delito, podrán ser recabados de los particulares en relación con sus clientes. No obstante, esto podría presentar algunos problemas en su aplicación, ya que la necesidad y proporcionalidad puede acreditarse con mayor contundencia cuando el requerimiento de datos se refiere a la investigación de un delito que se encuentra en curso, de manera que puede acreditarse que, como elemento de prueba, se requería el acceso a ciertos datos de cierta persona involucrada o relacionada directamente con dicha investigación, pero ¿qué sucede con las atribuciones genéricas de seguridad nacional, seguridad pública y prevención de los delitos? Aquí no necesariamente se estará ante una investigación abierta para un delito específico, por lo cual los extremos de la necesidad y proporcionalidad podrían ser más complicados de acreditar y los sujetos obligados podrían caer en excesos en cuanto a la cantidad de datos que busquen recabar, utilizando un argumento genérico de seguridad nacional o seguridad pública.[195]

[194] Como ejemplos podemos citar los Lineamientos de Colaboración en materia de Seguridad y Justicia, el artículo 5 de la Ley General del Sistema Nacional de Seguridad Pública, el artículo 6 de la Ley de Seguridad Nacional, así como las leyes que establecen las atribuciones de vigilancia a que hemos hecho referencia. También véase Amparo en revisión 964/2015. Disponible en: http://207.249.17.176/segundasala/asuntos%20lista%20oficial/AR-964-2015.pdf

[195] Análisis como el que articulan los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://necessaryandproportionate.

En ese sentido, los requerimientos de las autoridades con base en estas atribuciones deberán, caso por caso, acreditar la necesidad y proporcionalidad de conocer la información. Es por ello que, considerando que este tipo de datos —incluidos los metadatos a que hace referencia la Ley Federal de Telecomunicaciones— se refieren a la intervención de comunicaciones privadas en términos del artículo 16 constitucional, el análisis que realicen los jueces para la emisión de la orden judicial correspondiente se vuelve un elemento crucial en la debida acreditación de la necesidad y proporcionalidad. Asimismo, en el ámbito de la protección de datos, los organismos garantes deberán analizar el cumplimiento con dichos principios y los ciudadanos también podrán efectuar un seguimiento general al tema mediante las obligaciones e informes de transparencia, así como de solicitudes de acceso a información.

Asimismo, un tema muy importante será el acceso a los datos personales que requiera el propio titular, en relación con datos propios que hayan sido recabados por las autoridades, y la consiguiente acción que pueda ejercer frente a los organismos garantes dicho titular, a efecto de que se analice el cumplimiento con los mencionados principios, y en su caso, también poder solicitar su cancelación cuando los datos dejen de ser necesarios para el cumplimiento de los objetivos de la recolección. Cabe señalar, sin embargo, que este derecho por parte de los titulares resulta un tanto genérico, ya que se tendría que solicitar, prácticamente, a todas las autoridades involucradas en estos temas, conocer si se requirió información sobre dicho titular a alguna empresa privada.[196] Es por ello que el tema de notificación diferida se vuelve importante en esta materia, el cual consiste en informar a la persona cuyos datos fueron transferidos a las instancias de seguridad, procuración y administración de justicia —una vez que no se pone en riesgo la actividad que

org/principles, proporcionan elementos para promover legislaciones que ofrezcan verdaderas garantías para la ciudadanía y mejoren la seguridad jurídica sobre la que se deben basar las autoridades para hacer su trabajo. También véase Documento final de la reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información 2015. *Resolución A/70/125*. disponible en: http://unctad.org/es/PublicationsLibrary/ares70d125_es.pdf, que señala: "Recordamos la resolución 69/166 de la Asamblea General, y en este contexto recalcamos que nadie será objeto de injerencias arbitrarias o ilícitas en su vida privada, su familia, su domicilio o su correspondencia, en consonancia con las obligaciones que incumben a los países en virtud del derecho internacional de los derechos humanos. En consecuencia, exhortamos a todos los Estados a que revisen sus procedimientos, prácticas y legislación sobre vigilancia de las comunicaciones, así como su interceptación, y la reunión de datos personales, incluida la vigilancia en gran escala, con miras a afianzar el derecho a la privacidad, establecido en la Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos para los Estados que son parte en el Pacto, asegurando la aplicación plena y efectiva de todas las obligaciones que les incumben en virtud del derecho internacional de los derechos humanos".
También véase Electronic Frontier Foundation Privacy. *Mandatory Data Retention*, disponible en: https://www.eff.org/es/issues/mandatory-data-retention.

[196] Es importante notar que el titular de los datos también tiene expedita la vía para ejercer sus derechos ARCO directamente ante las empresas privadas que resguardan datos sobre dicho titular con base, por ejemplo, en los artículos 189 y 190 de la Ley Federal de Telecomunicaciones y Radiodifusión. Lo anterior, en términos de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

estuviera realizando el sujeto obligado correspondiente— que sus datos fueron entregados a dichas instancias, a efecto de que esté en posibilidad de ejercer sus derechos —en especial el de acceso y cancelación.[197] No obstante, esta obligación para las autoridades no fue incluida en el texto de la LGPDPPSO.

Por su parte, tal como deja claro el artículo 81 de esta ley, las instancias de seguridad y procuración de justicia deberán cumplir con los principios y deberes de protección de datos que establece la propia LGPDPPSO.

El Título Segundo de la ley desarrolla los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad, así como el deber de seguridad.[198]

Cabe señalar que en el caso de los datos personales que transfieren las empresas privadas a los sujetos obligados en materia de seguridad, procuración y administración de justicia, se encuentra exceptuado el principio de consentimiento, según se ha señalado anteriormente. Ello, en virtud de que el titular de los datos, cliente de la empresa privada, no tiene conocimiento y, por tanto, no proporciona su consentimiento para dicha transmisión. Esto tiene sentido si se piensa que la información puede estar relacionada con investigaciones en curso cuyo buen término requiere secrecía en la obtención de la información. Esta excepción al consentimiento encuentra su fundamento en el artículo 22, fracciones I y II de la LGPDPPSO:

> **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;
>
> […]

[197] Este derecho de notificación a las personas afectadas por medidas de vigilancia ha sido reconocido, por ejemplo, por el Relator Especial sobre el derecho a la libertad de opinión y expresión de la Organización de las Naciones Unidas. *A/HRC/23/40*, disponible en: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf. Párrafo 82: "Las personas deben tener el derecho a ser notificadas que han sido sujetas a la vigilancia de sus comunicaciones o bien, que los datos sobre sus comunicaciones han sido accedidos por el Estado. Si bien se reconoce que una notificación previa o concurrente podría poner en riesgo la efectividad de dicha vigilancia, lo cierto es que las personas deben ser notificadas una vez que la vigilancia ha sido completada a efecto de que estén en posibilidad de exigir restitución posterior respecto del uso de medidas de vigilancia de comunicaciones". (Traducción propia.)

[198] Un referente importante para la aplicación de los principios a este tipo de bases de datos lo constituyen los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponible en: https://necessaryandproportionate.org/principles.

**III.** Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;

Ahora bien, precisamente porque el titular de los datos no tiene conocimiento ni oportunidad de otorgar su consentimiento, sino que los datos son proporcionados por un tercero al sujeto obligado, es que resulta indispensable la oportunidad de ejercer el derecho de acceso, y en su caso, cancelación de los datos ante los sujetos obligados por parte del titular y obtener dicho acceso o cancelación una vez que la acción correspondiente que estuviera llevando a cabo la autoridad no se ponga en riesgo.

El segundo párrafo del artículo 81 de la LGPDPPSO reproduce lo señalado por el artículo 16 de la CPEUM en relación con la inviolabilidad de comunicaciones privadas. En este punto, cabe resaltar la discusión que se ha dado, específicamente en el tema de telecomunicaciones y los metadatos a que se refiere el artículo 190 de la Ley Federal de Telecomunicaciones y Radiodifusión, en relación con el hecho de que se requiera o no orden judicial para su solicitud por parte de las instancias de seguridad y justicia.[199]

[199] Los metadatos también se encuentran protegidos por el derecho a la inviolabilidad de comunicaciones, por tanto, las autoridades requieren orden judicial para poder solicitarlos. No obstante, respecto al dato relativo a la geolocalización en tiempo real, en México algunas interpretaciones han señalado que éste puede recabarse por instancias de seguridad y justicia sin necesidad de orden judicial, al no considerarlo parte de las comunicaciones privadas. Cfr. Acción de inconstitucionalidad 32/2012, presentada por la Comisión Nacional de los Derechos Humanos en contra del decreto por el cual "se reforman, adicionan y derogan diversas disposiciones del código federal de procedimientos penales, del código penal federal, de la ley federal de telecomunicaciones, de la ley que establece las normas mínimas sobre readaptación social de sentenciados y de la ley general del sistema nacional de seguridad pública". Disponible en: www2.scjn.gob.mx/juridica/engroses/cerrados/Publico/12000320.019-2032.doc
También véase el *Amparo en revisión 964/2015* en el que se establece que: "[…] la protección de la inviolabilidad de las comunicaciones, puede comprender tanto el contenido de las comunicaciones, como aquellos datos que permitan identificarlas —metadatos— pues del análisis de los datos de tráfico de comunicaciones se pueden extraer conclusiones muy precisas sobre la vida privada de las personas cuya información se han conservado, como lo pueden ser los hábitos de la vida cotidiana, las actividades realizadas y las relaciones personales, entre otras…[sin embargo] la localización geográfica, en tiempo real, de los equipos de comunicación móvil, no se traduce en una violación del derecho fundamental a la inviolabilidad de las comunicaciones, en virtud de que, como se ha determinado, dicha medida no se dirige a la persona ni se relaciona con la obtención de alguna información relacionada con las comunicaciones o alguno de sus procesos comunicativos —metadatos— sino que se contrae a la ubicación del lugar en el momento preciso en que se procesa la búsqueda, de un equipo terminal móvil, asociado a una línea telefónica determinada, es decir, no se proyecta hacia la esfera de la íntimo o lo privado de los gobernados, y por tanto, no transgrede el referido derecho humano". Disponible en: http://207.249.17.176/segundasala/asuntos%20lista%20oficial/AR-964-2015.pdf
Sin embargo, el artículo 303 del Código Nacional de Procedimientos Penales (reformado en 2016) sí requiere autorización judicial aun para el dato de geolocalización en tiempo real: "Artículo 291. Intervención de las comunicaciones privadas. Cuando en la investigación el Ministerio Público considere necesaria la intervención de comunicaciones privadas, el Titular de la Procuraduría General de la República, o en quienes éste delegue esta facultad, así como los Procuradores de las entidades federativas, podrán solicitar al Juez federal de control competente, por cualquier medio, la autorización para practicar la intervención, expresando el objeto y necesidad de la misma.
La intervención de comunicaciones privadas, abarca todo sistema de comunicación, o programas que sean resultado de la evolución tecnológica, que permitan el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos que graben, conserven el

El artículo 82 reproduce el artículo 31 de la propia LGPDPPSO, y como se ha dicho, los sujetos obligados deben cumplir con todo el capítulo relativo al deber de seguridad. El elemento nuevo que inserta tiene que ver con la obligación de establecer medidas de seguridad *de nivel alto*.[200] Esta obligación

contenido de las conversaciones o registren datos que identifiquen la comunicación, los cuales se pueden presentar en tiempo real.
La solicitud deberá ser resuelta por la autoridad judicial de manera inmediata, por cualquier medio que garantice su autenticidad, o en audiencia privada con la sola comparecencia del Ministerio Público, en un plazo que no exceda de las seis horas siguientes a que la haya recibido. También se requerirá autorización judicial en los casos de extracción de información, la cual consiste en la obtención de comunicaciones privadas, datos de identificación de las comunicaciones; así como la información, documentos, archivos de texto, audio, imagen o video contenidos en cualquier dispositivo, accesorio, aparato electrónico, equipo informático, aparato de almacenamiento y todo aquello que pueda contener información, incluyendo la almacenada en las plataformas o centros de datos remotos vinculados con éstos…
Artículo 303. Localización geográfica en tiempo real y solicitud de entrega de datos conservados.
Cuando el Ministerio Público considere necesaria la localización geográfica en tiempo real o entrega de datos conservados por los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos de los equipos de comunicación móvil asociados a una línea que se encuentra relacionada con los hechos que se investigan, el Procurador, o el servidor público en quien se delegue la facultad, podrá solicitar al Juez de control del fuero correspondiente en su caso, por cualquier medio, requiera a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, para que proporcionen con la oportunidad y suficiencia necesaria a la autoridad investigadora, la información solicitada para el inmediato desahogo de dichos actos de investigación. Los datos conservados a que refiere este párrafo se destruirán en caso de que no constituyan medio de prueba idóneo o pertinente. En la solicitud se expresarán los equipos de comunicación móvil relacionados con los hechos que se investigan, señalando los motivos e indicios que sustentan la necesidad de la localización geográfica en tiempo real o la entrega de los datos conservados, su duración y, en su caso, la denominación de la empresa autorizada o proveedora del servicio de telecomunicaciones a través del cual se operan las líneas, números o aparatos que serán objeto de la medida…Excepcionalmente, cuando esté en peligro la integridad física o la vida de una persona o se encuentre en riesgo el objeto del delito, así como en hechos relacionados con la privación ilegal de la libertad, secuestro, extorsión o delincuencia organizada, el Procurador, o el servidor público en quien se delegue la facultad, bajo su más estricta responsabilidad, ordenará directamente la localización geográfica en tiempo real o la entrega de los datos conservados a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos, quienes deberán atenderla de inmediato y con la suficiencia necesaria…Cuando el Juez de control no ratifique la medida a que hace referencia el párrafo anterior, la información obtenida no podrá ser incorporada al procedimiento penal. Asimismo el Procurador, o el servidor público en quien se delegue la facultad podrá requerir a los sujetos obligados que establece la Ley Federal de Telecomunicaciones y Radiodifusión, la conservación inmediata de datos contenidos en redes, sistemas o equipos de informática, hasta por un tiempo máximo de noventa días, lo cual deberá realizarse de forma inmediata. La solicitud y entrega de los datos contenidos en redes, sistemas o equipos de informática se llevará a cabo de conformidad por lo previsto por este artículo. Lo anterior sin menoscabo de las obligaciones previstas en materia de conservación de información para las concesionarias y autorizados de telecomunicaciones en términos del artículo 190, fracción II de la Ley Federal de Telecomunicaciones y Radiodifusión".
Asimismo, véase Grupo de Trabajo sobre Protección de Datos Artículo 29. (2011). *Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes*. [Archivo PDF]. Disponible en: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf, [fecha de consulta: 5 de mayo 2018].

[200] Podrán tomarse en cuenta los diversos instrumentos que guían el establecimiento de medidas de seguridad, tal como las *Recomendaciones en materia de seguridad de datos personales y la Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales*, ambos expedidos por el Instituto Federal de Acceso a la Información y Protección de Datos (ahora INAI). Disponible en: http://www.dof.gob.mx/nota_detalle_popup.php?codigo=5320179 y https://sontusdatos.org/wp-content/uploads/2013/04/ifai-guia-implementacion-sistema-de-gestion-de-seguridad-datos-personales_2014.pdf

resulta pertinente toda vez que se trata de datos que el titular no proporcionó de manera directa al sujeto obligado y que, además, se relacionan con las materias de seguridad nacional, seguridad pública y persecución de los delitos. Asimismo, toda vez que, con base en estas atribuciones, las instancias gubernamentales podrían estar generando bases de datos paralelas a las que detenta el sector privado, dichas bases de datos deben contar con medidas de seguridad suficientes, de lo contrario, se aumentan las vulnerabilidades y la posibilidad de que personas no autorizadas tengan acceso a los datos. Aunado a ello, es una paradoja que estas bases de datos generen perfiles de los individuos que, de caer en manos del crimen organizado, facilitarían sus actividades ilícitas poniendo en riesgo la integridad de las personas.

Por último, si bien no es parte del capítulo en análisis, es necesario resaltar que en el apartado de la LGPDPPSO que regula las facultades de verificación del INAI y de los organismos garantes se establece lo siguiente:

> **Artículo 149.** La verificación iniciará mediante una orden escrita que funde y motive la procedencia de la actuación por parte del Instituto o de los Organismos garantes, la cual tiene por objeto requerir al responsable la documentación e información necesaria vinculada con la presunta violación y/o realizar visitas a las oficinas o instalaciones del responsable, o en su caso, en el lugar donde estén ubicadas las bases de datos personales respectivas.
>
> **Para la verificación en instancias de seguridad nacional y seguridad pública, se requerirá en la resolución, la aprobación del Pleno del Instituto, por mayoría calificada de sus Comisionados, o de los integrantes de los Organismos garantes de las Entidades Federativas, según corresponda; así como de una fundamentación y motivación reforzada de la causa del procedimiento, debiéndose asegurar la información sólo para uso exclusivo de la autoridad y para los fines establecidos en el artículo 150.**[201]

Como puede observarse, para las verificaciones que se realicen a las instancias de seguridad nacional y seguridad pública se establecen requisitos adicionales que deberán cumplir el INAI y los organismos garantes para poder ejercer esta atribución, atendiendo a las funciones y atribuciones de las mencionadas instancias.

[201] Texto resaltado por la autora.

## IV. Conclusiones

Si bien la inserción del capítulo analizado es importante por las razones expuestas, lo cierto es que existen temas que pudieron haberse incluido y que permitirían robustecer los criterios que deberán aplicar las autoridades en el uso de estas atribuciones, así como establecer mayores mecanismos de control por parte de la ciudadanía y de los titulares de los datos.

Algunos de los temas que quedan pendientes para alguna futura reforma o como temas por analizar en posibles criterios de interpretación de los organismos garantes, son:

1. El carácter residual de la retención de datos frente a otras técnicas menos invasivas como criterio de interpretación para los principios de proporcionalidad y necesidad de conocer (licitud).

2. El de notificación diferida al titular de los datos —una vez que no se ponga en riesgo la actividad que estuviera realizando el sujeto obligado correspondiente— a efecto de que esté en posibilidad de ejercer sus derechos —en especial el de acceso y cancelación— a partir de la certeza de que fueron recabados por una instancia de seguridad y justicia.

3. Claridad en cuanto a los límites para ulteriores transferencias que pueda realizar el sujeto obligado a otras autoridades.

4. El tipo de delitos cuya investigación permite solicitar este tipo de información (por ejemplo, para delitos graves).

5. Criterios para acotar las funciones de seguridad nacional, seguridad pública y prevención del delito, cuando dichas funciones no se relacionan con una investigación concreta en curso.

6. Sanción específica por el incumplimiento de alguna de las disposiciones del capítulo respectivo, o por la divulgación o comercialización indebida de los datos por parte de las instancias de seguridad y justicia.

7. Análisis de los informes que se presentan al Instituto Federal de Telecomunicaciones por parte de autoridades y de empresas privadas.

8. Análisis del debido cumplimiento de obligaciones de transparencia en este tema.

Como corolario, cabe destacar lo señalado por el Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión y la Relatora Especial para la Libertad

de Expresión de la Comisión Interamericana de Derechos Humanos de la Organización de los Estados Americanos (OEA) en la Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión:

> […] los Estados deben garantizar que la intervención, recolección y uso de información personal, incluidas todas las limitaciones al derecho de la persona afectada a acceder a información sobre las mismas, estén claramente autorizadas por la ley a fin de proteger a la persona contra interferencias arbitrarias o abusivas en sus intereses privados. La ley deberá establecer límites respecto a la naturaleza, alcance y duración de este tipo de medidas, las razones para ordenarlas, las autoridades competentes para autorizar, ejecutar y supervisarlas y los mecanismos legales para su impugnación.
>
> Dada la importancia del ejercicio de estos derechos para el sistema democrático, la ley debe autorizar el acceso a las comunicaciones y a datos personales sólo en las circunstancias más excepcionales definidas en la legislación. Cuando se invoque la seguridad nacional como razón para vigilar la correspondencia y los datos personales, la ley debe especificar claramente los criterios que deben aplicarse para determinar los casos en los cuales este tipo de limitaciones resulta legítimo. Su aplicación deberá autorizarse únicamente cuando exista un riesgo cierto respecto de los intereses protegidos, y cuando ese daño sea superior al interés general de la sociedad en función de mantener el derecho a la privacidad y a la libre expresión del pensamiento y circulación de información. La entrega de esta información debe ser monitoreada por un organismo de control independiente y contar con garantías suficientes de debido proceso y supervisión judicial, dentro de las limitaciones permisibles en una sociedad democrática.[202]

[202] Declaración Conjunta sobre Programas de Vigilancia y su Impacto en la Libertad de Expresión, Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión y la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA. Disponible en: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=927

## Referencias

Asamblea General de las Naciones Unidas. (2013). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. [Archivo PDF].Disponible en: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf, [fecha de consulta: 5 de mayo 2018].

Asamblea General de las Naciones Unidas. (2015). *Documento final de la reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información*. [Archivo PDF]. Disponible en: http://unctad.org/es/PublicationsLibrary/ares70d125_es.pdf

Cámara de Diputados. (2014). *Código Nacional de Procedimientos Penales. Diario Oficial de la Federación*. [Archivo PDF]. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_170616.pdf, [fecha de consulta: 5 de mayo 2018].

Cámara de Diputados. (2016). *Dictamen que emite la Comisión de Transparencia y Anticorrupción de la Cámara de Diputados con relación a la Minuta con Proyecto de Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*. [Archivo PDF]. Disponible en: https://sontusdatos.org/wp-content/uploads/2016/11/Dictamen-LGPDP-en-t%C3%A9rminos-de-la-Minuta-Datos-Personales-2.pdf, [fecha de consulta: 5 de mayo 2018].

DOF. (2014). Ley Federal de Telecomunicaciones y Radiodifusión, *Diario Oficial de la Federación*. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5352323&fecha=14/07/2014, [fecha de consulta: 5 de mayo 2018].

DOF. (2015). Ley General de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*. [Archivo PDF]. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP.pdf, [fecha de consulta: 5 de mayo 2018].

DOF. (2016). Ley Federal de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*. [Archivo PDF]. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_270117.pdf, [fecha de consulta: 5 de mayo 2018].

Electronic Frontier Foundation. (s.f.). *Mandatory Data Retention*. Disponible en: https://www.eff.org/es/issues/mandatory-data-retention, [fecha de consulta: 5 de mayo 2018].

Google, Inc. (2017). *Informe de transparencia*. Disponible en: https://transparencyreport.google.com/, y https://www.youtube.com/watch?v=MeKKHxcJfh0, [fecha de consulta: 5 de mayo 2018].

Grupo de Trabajo del Artículo 29. (2011). *Dictamen 13/2011 sobre los servicios de geolocalización en los dispositivos móviles inteligentes*. [Archivo PDF]. Disponible en: https://www.apda.ad/system/files/wp185_es.pdf, [fecha de consulta: 5 de mayo 2018].

Instituto Federal de Transparencia, Acceso a la Información y Protección de Datos. (2013). Recomendaciones en materia de seguridad de datos personales, *Diario Oficial de la Federación*. Disponible en: http://www.dof.gob.mx/nota_detalle_popup.php?codigo=5320179, [fecha de consulta: 5 de mayo 2018].

Instituto Federal de Transparencia, Acceso a la Información y Protección de Datos. (2014). *Guía para implementar un Sistema de Gestión de Seguridad de Datos Personales*. [Archivo PDF]. Disponible en: https://sontusdatos.org/wp-content/uploads/2013/04/ifai-guia-implementacion-sistema-de-gestion-de-seguridad-datos-personales_2014.pdf, [fecha de consulta: 5 de mayo 2018].

Instituto Federal de Telecomunicaciones. (2015). Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones expide los Lineamientos de Colaboración en materia de Seguridad y Justicia y modifica el Plan Técnico fundamental de numeración, *Diario Oficial de la Federación*. Disponible en: http://www.dof.gob.mx/nota_detalle.php?codigo=5418339&fecha=02/12/2015, [fecha de consulta: 5 de mayo 2018].

Microsoft. (2017). *Corporate Social Responsability Report*. Disponible en: https://www.microsoft.com/en-us/about/corporate-responsibility/reports-hub, [fecha de consulta: 5 de mayo 2018].

Necessary and Proportionate Coalition. (2014). *Necessary and Proportionate, International Principles on the Application of Human Rights to Communications Surveillance*. Disponible en: https://necessaryandproportionate.org/principles, [fecha de consulta: 5 de mayo 2018].

Office of the United Nations High Commissioner for Human Rights. (2013). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. [Archivo PDF]. Disponible en: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

Organización de los Estados Americanos. (2013). *Relator Especial de las Naciones Unidas (ONU) para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión y la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA*. Disponible en: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=927, [fecha de consulta: 5 de mayo 2018].

Piñar, J. y Ornelas, L. (Coords.). (2013). *La protección de datos personales en México*. México: Tirant Lo Blanch.

Red en Defensa de los Derechos Digitales (R3D). (2016). *¿Quién defiende tus datos? 2016*. Disponible en: https://r3d.mx/wp-content/uploads/QDTD2016_v02_WEB.pdf y https://r3d.mx/2016/12/13/qdtd2016/, [fecha de consulta: 5 de mayo 2018].

Red en Defensa de los Derechos Digitales (R3D). (2016). *El Estado de la Vigilancia, Fuera de Control*. México: R3D, p. 17. [Archivo PDF]. Disponible en: https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016-FINAL1.pdf, [fecha de consulta: 5 de mayo 2018].

Senado de la República. (2013). *Dictamen de las Comisiones Unidas de Anticorrupción y Participación Ciudadana, de Gobernación y de Estudios Legislativos, Segunda del Senado de la República; relativo a la iniciativa que contiene Proyecto de Decreto por el que se expide la Ley General de Transparencia y Acceso a la Información Pública*. Disponible en: http://rendiciondecuentas.org.mx/wp-content/uploads/2015/03/Dictam-en-Transparencia-Aprobado-2013.03.18.pdf, [fecha de consulta: 5 de mayo 2018].

Suprema Corte de Justicia de la Nación. *Acción de inconstitucionalidad 32/2012*. Disponible en: https://www.sitios.scjn.gob.mx/video/?q=category/expediente/acci%C3%B3n-de-inconstitucionalidad-322012

Suprema Corte de Justicia de la Nación. (2015). *Amparo en revisión 964/2015*. [Archivo PDF]. Disponible en: http://207.249.17.176/segundasala/asuntos%20lista%20oficial/AR-964-2015.pdf, [fecha de consulta: 5 de mayo 2018].

Tribunal de Justicia de la Unión Europea. (2014). *Comunicado de prensa núm. 54/14.* [Archivo PDF]. Disponible en: https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054es.pdf, [fecha de consulta: 5 de mayo 2018].

# TÍTULO SÉPTIMO

# RESPONSABLES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS SUJETOS OBLIGADOS

# CAPÍTULO I
# COMITÉ DE TRANSPARENCIA

***Artículo 83.*** *Cada responsable contará con un Comité de Transparencia, el cual se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable.*

*El Comité de Transparencia será la autoridad máxima en materia de protección de datos personales.*

***Artículo 84.*** *Para los efectos de la presente Ley y sin perjuicio de otras atribuciones que le sean conferidas en la normatividad que le resulte aplicable, el Comité de Transparencia tendrá las siguientes funciones:*

*I. Coordinar, supervisar y realizar las acciones necesarias para garantizar el derecho a la protección de los datos personales en la organización del responsable, de conformidad con las disposiciones previstas en la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;*

*II. Instituir, en su caso, procedimientos internos para asegurar la mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;*

*III. Confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales, o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO;*

*IV. Establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la presente Ley y en aquellas disposiciones que resulten aplicables en la materia;*

*V. Supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad;*

*VI. Dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto y los organismos garantes, según corresponda;*

*VII. Establecer programas de capacitación y actualización para los servidores públicos en materia de protección de datos personales, y*

*VIII. Dar vista al órgano interno de control o instancia equivalente en aquellos casos en que tenga conocimiento, en el ejercicio de sus atribuciones, de una presunta irregularidad respecto de determinado tratamiento de datos personales; particularmente en casos relacionados con la declaración de inexistencia que realicen los responsables.*

## COMENTARIO

**Jimena Moreno González**

### I. Antecedentes

En el artículo 29 de la LFTAIPG, publicada en el *Diario Oficial de la Federación* el 11 de junio de 2002, se preveía que cada dependencia tuviera un Comité de Información cuyas funciones estaban básicamente dirigidas a: a) coordinar, gestionar y supervisar las acciones para proporcionar información; b) confirmar, modificar o revocar la clasificación de la información, y c) establecer y supervisar la aplicación de criterios específicos en materia de clasificación y conservación de archivos. Este Comité debía estar integrado por un servidor público, el titular de la Unidad de Enlace y el titular del Órgano Interno de Control de cada dependencia o entidad (artículo 30).

En la exposición de motivos de la abrogada LFTAIPG, se establecía que "el esquema est[aba] diseñado para evitar que el particular transite por innumerables oficinas administrativas o bien, que tenga que conocer forzosamente la ubicación de la unidad en que físicamente se encuentre la documentación solicitada. Es decir, él recibe toda la atención y la tramitación de su solicitud, hasta que se le dé respuesta, en la ventanilla de acceso".[203]

Es hasta la emisión de la nueva Ley Federal de Transparencia y Acceso a la Información Pública del 9 de mayo de 2016, donde se cambia de Comité de Información a Comité de Transparencia, con facultades más amplias y funciones más específicas.

[203] "Dictamen de la Comisión de Gobernación y Seguridad Pública, con proyecto de Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental". *Proyecto de Decreto de Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*, de 22 de abril de 2002.

## II. Relevancia temática y contexto

El Comité de Transparencia desde su creación fue diseñado como un comité colegiado cuyas funciones principales son revisar la información que se produzca en las áreas, para garantizar tanto el derecho de acceso a la información como el derecho a la protección de datos personales. Además, en materia de datos personales es la autoridad máxima y es la responsable de proteger y garantizar los derechos ARCO por parte del sujeto obligado.

Por lo anterior, el Comité es una instancia de gran relevancia y cuya conformación, en el contexto de una sociedad democrática y abierta en la que se deben de tener datos accesibles y a disposición de la sociedad, es indispensable para garantizar la no divulgación de los datos personales y los datos personales sensibles tanto de los titulares como de terceros.

## III. Análisis del contenido

El Comité de Transparencia está regulado en los artículos 83 y 84 de esta ley. El artículo 83 mandata la creación de un Comité de Transparencia para los responsables del tratamiento de datos personales que recae en los sujetos obligados señalados en el artículo primero, párrafo cuarto de la ley.[204] La conformación y funcionamiento del Comité de Transparencia está regulada de manera genérica en los artículos 43 y 44 de la Ley General de Transparencia y Acceso a la Información Pública (en adelante LGTAIP). Específicamente, el Capítulo III De los Comités de Transparencia de la LGTAIP, es el que prescribe las funciones y facultades del Comité que es el responsable de verificar la clasificación de la información y de supervisar todo lo relativo a las solicitudes de acceso en la misma institución, así como el responsable de confirmar, modificar o revocar la clasificación de la información que hubieran hecho los titulares de las unidades administrativas.

De acuerdo con la LGTAIP, este Comité deberá ser colegiado, integrado por número impar, sus integrantes no podrán depender jerárquicamente entre sí, ni podrán reunirse dos o más personas de los integrantes en una sola persona y sus resoluciones son por mayoría de votos. En caso de empate, el presidente tiene voto de calidad. Este diseño obedece a la preocupación que existía en el sentido de que los integrantes del Comité no tuvieran libertad, ni estuvieran sujetos a presiones en el momento de clasificar la información y

[204] Artículo 1. "[…] son sujetos obligados por esta Ley, en el ámbito federal, estatal y municipal, cualquier autoridad , entidad, órganos y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos púbicos.
Los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en al 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".

con la intención de hacer un comité imparcial e independiente de intereses de superiores jerárquicos.

Es importante tener en cuenta que el artículo 43, párrafo cuarto de la LGTAIP dispone que el tratamiento de información que involucra aspectos de seguridad nacional, combate a la delincuencia, protección de personas, investigaciones referentes a inteligencia financiera, competencia económica y de telecomunicaciones no estará sujeto a la autoridad del Comité de Transparencia.[205]

Como se mencionó anteriormente, la creación del Comité ya estaba prevista en la abrogada LFTAIPG del 11 de junio de 2002 en la que se establecieron, en el artículo 29, las funciones del Comité y en el artículo 30 su conformación, la cual estaba prescrita de la siguiente manera: "Cada Comité estará integrado por: I. Un servidor público designado por el titular de la dependencia o entidad; II. El titular de la unidad de enlace, y III. El titular del órgano interno de control de cada dependencia o entidad".

Sin embargo, en el artículo 64 de la vigente LFTAIP se cambia la conformación de dicho Comité para que quede integrado por el responsable del área coordinadora de archivos o equivalente y los titulares de la Unidad de Transparencia y del Órgano Interno de Control de cada dependencia o entidad.

Por ello, y para hacer más expedita esta búsqueda, se considera que un miembro importante del Comité es el encargado de archivos del sujeto obligado ya que, conforme al esquema diseñado para cumplir con las obligaciones en materia de transparencia y protección de datos, es una forma de facilitar la obtención, recuperación o declarar la inexistencia de la información. Lo cual se deduce de la exposición de motivos de la LGTAIP, ya que a pesar de que no se da una explicación clara y concreta sobre la razón por la que se decidió integrar al encargado de archivos en el Comité, sí se infiere esa necesidad a partir de las facultades ya expuestas.[206]

---

[205] "El Centro de Investigación y Seguridad Nacional; el Centro Nacional de Planeación, Análisis e Información para el Combate a la Delincuencia; el Centro Federal de Protección a Personas; la Dirección de Coordinación de Inteligencia de la Comisión Nacional de Seguridad; la Subprocuraduría Especializada en Investigación de Delincuencia Organizada; la Unidad de Inteligencia Financiera; el Estado Mayor Presidencial, el Estado Mayor de la Defensa Nacional, el Estado Mayor General de la Armada, la Autoridad Investigadora de la Comisión Federal de Competencia Económica y la del Instituto Federal de Telecomunicaciones o bien, las unidades administrativas que los sustituyan, no estarán sujetos a la autoridad de los Comités de Transparencia a que se refiere el presente Artículo, siendo sus funciones responsabilidad exclusiva del titular de la propia entidad o unidad administrativa.
La clasificación, desclasificación y acceso a la información que generen o custodien las instancias de inteligencia e investigación deberá apegarse a los términos previstos en la presente Ley y a los protocolos de seguridad y resguardo establecidos para ello".

[206] Ver Senado de la República. (2015). *Dictamen de las Comisiones Unidas de Anticorrupción y Participación Ciudadana, de Gobernación y de Estudios Legislativos, Segunda; Relativo a la Iniciativa que contiene Proyecto de Decreto por el que se expide la Ley General de Transparencia*

El artículo 24 de la LGTAIP también explica que los sujetos obligados deberán constituir el Comité de Transparencia y las Unidades de Transparencia y designar al titular de cada una de las unidades de Transparencia (quienes, preferentemente, deberán tener experiencia en la materia), así como proporcionar capacitación continua al personal que los integre.

Tal como lo indica el segundo párrafo del artículo 83, el Comité de Transparencia es la "autoridad máxima en materia de protección de datos personales". Esto permite dotarlo de autonomía, característica fundamental para su funcionamiento y para emitir resoluciones en materia de datos personales. Además, la ley le permite y deja al arbitrio del mismo, la creación de sus procedimientos internos para desempeñar cada una de las funciones contenidas en el artículo 84 y allegarse de expertos que tienen voz, pero no voto.

Por su parte el artículo 84 de la LGPDPPSO establece las funciones del Comité de Transparencia, las cuales también están señaladas en el artículo 44 de la LGTAIP. Sus funciones atienden a gestionar solicitudes de acceso a la información dentro de las áreas responsables de cada institución y es la instancia responsable para contestar las solicitudes de acceso ante los solicitantes como ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Las labores más relevantes del Comité son: clasificar la información y declarar la inexistencia o la incompetencia de los titulares de las áreas respecto a una solicitud de información.[207]

---

*y Acceso a La Información Pública*, p. 17. [Archivo PDF]. Disponible en: http://rendiciondecuentas.org.mx/wp-content/uploads/2015/03/Dictam-en-Transparencia-Aprobado-2013.03.18.pdf, [fecha de consulta: 6 de mayo 2018].

[207] "Artículo 44. Cada Comité de Transparencia tendrá las siguientes funciones:
I. Instituir, coordinar y supervisar, en términos de las disposiciones aplicables, las acciones y los procedimientos para asegurar la mayor eficacia en la gestión de las solicitudes en materia de acceso a la información;
II. Confirmar, modificar o revocar las determinaciones que en materia de ampliación del plazo de respuesta, clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las Áreas de los sujetos obligados;
III. Ordenar, en su caso, a las Áreas competentes que generen la información que derivado de sus facultades, competencias y funciones deban tener en posesión o que previa acreditación de la imposibilidad de su generación, exponga, de forma fundada y motivada, las razones por las cuales, en el caso particular, no ejercieron dichas facultades, competencias o funciones;
IV. Establecer políticas para facilitar la obtención de información y el ejercicio del derecho de acceso a la información;
V. Promover la capacitación y actualización de los Servidores Públicos o integrantes adscritos a las Unidades de Transparencia;
VI. Establecer programas de capacitación en materia de transparencia, acceso a la información, accesibilidad y Protección de datos personales, para todos los Servidores Públicos o integrantes del sujeto obligado;
VII. Recabar y enviar al organismo garante, de conformidad con los lineamientos que estos expidan, los datos necesarios para la elaboración del informe anual;
VIII. Solicitar y autorizar la ampliación del plazo de reserva de la información a que se refiere el Artículo 101 de la presente Ley, y
IX. Las demás que se desprendan de la normatividad aplicable".

El Comité de Transparencia es la figura más relevante en la procuración de procedimientos sencillos y expeditos para que los particulares puedan ejercer los derechos ARCO, posibilitando, de esta manera, la autodeterminación informativa, ya que es el área mediante la cual se realizan las acciones necesarias para dar cumplimiento al ejercicio del derecho que tiene toda persona a la protección de sus datos personales en posesión de sujetos obligados. Así, el Comité de Transparencia no sólo aplica esta ley directamente, sino que también hace un ejercicio de interpretación de la misma al determinar cuándo se está ante un dato personal, un dato personal sensible, la forma de protegerlos y el nivel de protección que deben tener.

Asimismo, para la atención de las facultades de este Comité para declarar la inexistencia y ordenar la generación de la información derivada de las competencias y funciones de los sujetos obligados y que poseen en sus archivos, el Comité debe tomar las medidas necesarias para la localización de la información, pues únicamente de esta manera es como puede hacer una resolución motivada y fundada de la clasificación de información confidencial o reservada o de su inexistencia.

En esta clasificación es donde la protección de datos tiene lugar, además de lo que indica la misma LGPDPPSO, pues, en gran medida, las unidades administrativas, al dar una respuesta a las solicitudes de información, tienen que realizar la clasificación de la misma y, en su caso, las versiones públicas de dicha información, las cuales deben ser confirmadas, modificadas o revocadas por el Comité de Transparencia. Por lo que, en mayor medida, la protección de datos se da a partir de una solicitud de información regida por la LGTAIP y la LFTAIP, pues el procedimiento administrativo por medio del cual se realizan estas acciones y los medios de defensa que interponen los particulares los conoce y resuelve el Pleno. Por lo que la confirmación, modificación o revocación de la clasificación de la información es una de las facultades más importantes del Comité.

Como se mencionó en el párrafo anterior, una de las funciones más importantes del Comité está contenida en la fracción III y es la relativa a la facultad que tiene para confirmar, modificar o revocar las determinaciones en las que se declare la inexistencia de los datos personales o se niegue por cualquier causa el ejercicio de alguno de los derechos ARCO. Es decir, el Comité es la única instancia que emite una determinación sobre la inexistencia de datos o la razón por la que se niegan. Es relevante señalar que el Comité tiene la facultad de negar la cancelación de los datos personales a un particular por cuestiones de interés público ejerciendo así la facultad de limitar este derecho.

De acuerdo con la fracción IV, el Comité tiene la facultad para establecer y supervisar la aplicación de criterios específicos que resulten necesarios para una mejor observancia de la presente ley y en aquellas disposiciones que resulten aplicables en la materia. Es aquí, donde se vuelve fundamental la capacidad de interpretación de la ley y de la emisión de los criterios aplicables de los miembros del Comité.

La fracción V mandata la obligación de supervisar, en coordinación con las áreas o unidades administrativas competentes, el cumplimiento de las medidas, controles y acciones previstas en el documento de seguridad, el cual es el instrumento que describe y da cuenta, de manera general, sobre las medidas de seguridad técnicas, físicas y administrativas adoptadas por el responsable para garantizar la confidencialidad, integridad y disponibilidad de los datos personales que posee. Es decir, deberá estar atento a las medidas de seguridad para evitar la sustracción de información que contenga datos personales y para el caso de datos sensibles, también supervisar que estos estándares de seguridad sean mayores.

El Comité también es el encargado de dar seguimiento y cumplimiento a las resoluciones emitidas por el Instituto y los organismos garantes, según corresponda, así lo dispone la fracción VI.

## IV. Conclusiones

El Comité de Transparencia, dentro de las instituciones públicas, se ha convertido en la figura rectora y garante del derecho a la información y del derecho a la protección de datos personales. El cambio en su integración para incluir al responsable de archivos permite que se agilice la búsqueda de información. Sin embargo, es importante mencionar que los integrantes del mismo deben conocer y estar capacitados en la materia. Es decir, se deben capacitar y profesionalizar debido a que son la autoridad máxima en datos personales y se convierten en el garante de los mismos. La elaboración de versiones públicas y la declaración de la información como reservada o confidencial requiere conocimiento y técnica de argumentación que justifique su resguardo como excepción al principio de máxima publicidad consagrado en el artículo 6º de la Constitución Política de los Estados Unidos Mexicanos.

## Referencias

Cámara de Diputados. (2002). *Dictamen de la Comisión de Gobernación y Seguridad Pública, con proyecto de Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Proyecto de Decreto de Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*.

DOF. (2002). Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, *Diario Oficial de la Federación*.

DOF. (2015). Ley General de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*.

DOF. (2016). Ley Federal de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*.

Senado de la República. (2015). *Dictamen de las Comisiones Unidas de Anticorrupción y Participación Ciudadana, de Gobernación y de Estudios Legislativos, Segunda; Relativo a la Iniciativa que contiene Proyecto de Decreto por el que se expide la Ley General de Transparencia y Acceso a la Información Pública*, p. 17. [Archivo PDF]. Disponible en: http://rendiciondecuentas.org.mx/wp-content/uploads/2015/03/Dictam-en-Transparencia-Aprobado-2013.03.18.pdf, [fecha de consulta: 6 de mayo 2018].

# CAPÍTULO II
# DE LA UNIDAD DE TRANSPARENCIA

***Artículo 85.*** *Cada responsable contará con una Unidad de Transparencia, se integrará y funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública, esta Ley y demás normativa aplicable, que tendrá las siguientes funciones:*

*I. Auxiliar y orientar al titular que lo requiera con relación al ejercicio del derecho a la protección de datos personales;*

*II. Gestionar las solicitudes para el ejercicio de los derechos ARCO;*

*III. Establecer mecanismos para asegurar que los datos personales solo se entreguen a su titular o su representante debidamente acreditados;*

*IV. Informar al titular o su representante el monto de los costos a cubrir por la reproducción y envío de los datos personales, con base en lo establecido en las disposiciones normativas aplicables;*

*V. Proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO;*

*VI. Aplicar instrumentos de evaluación de calidad sobre la gestión de las solicitudes para el ejercicio de los derechos ARCO, y*

*VII. Asesorar a las áreas adscritas al responsable en materia de protección de datos personales.*

*Los responsables que en el ejercicio de sus funciones sustantivas lleven a cabo tratamientos de datos personales relevantes o intensivos, podrán designar a un oficial de protección de datos personales, especializado en la materia, quien realizará las atribuciones mencionadas en este artículo y formará parte de la Unidad de Transparencia.*

*Los sujetos obligados promoverán acuerdos con instituciones públicas especializadas que pudieran auxiliarles a la recepción, trámite y entrega de*

*las respuestas a solicitudes de información, en la lengua indígena, braille o cualquier formato accesible correspondiente, en forma más eficiente.*

***Artículo 86.*** *El responsable procurará que las personas con algún tipo de discapacidad o grupos vulnerables, puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales.*

***Artículo 87.*** *En la designación del titular de la Unidad de Transparencia, el responsable estará a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable.*

## COMENTARIO

**Jimena Moreno González**

### I. Antecedentes

En el artículo 28 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTPAIPG), publicada en el *Diario Oficial de la Federación* el 11 de junio de 2002, se preveía que el titular de cada dependencia designara al titular de la Unidad de Enlace cuyas funciones estaban básicamente dirigidas a dar cumplimiento a las obligaciones de transparencia, a recibir y dar trámite a las solicitudes de acceso a la información, a llevar un registro de las mismas y a agilizar los trámites internos para entregar la información en tiempo y forma.

En la exposición de motivos de la abrogada LFTAIPG, se explicaba la naturaleza de la Unidad y se establecía el procedimiento de acceso a la información de la Administración Pública Federal para lo cual se creaban dos instancias: el Comité de Información y la Unidad de Enlace. Para efectos de este comentario sólo me referiré a la Unidad de Enlace.

De conformidad con el Dictamen emitido por la Comisión de Gobernación y Seguridad Pública de la Cámara de Diputados, mismo en el que se contenía el proyecto de la LFTAIPG, del 22 de abril de 2002, la Unidad de Enlace “es la encargada de ser el vínculo entre los particulares y la propia dependencia. Esta Unidad deberá recibir y dar trámite a las solicitudes que se presenten, realizar lo necesario para entregar la información solicitada, y llevar un registro de las solicitudes atendidas, entre otras”. Esta Unidad se diseñó para ser el primer contacto con los particulares no sólo para dar trámite y seguimiento a las solicitudes de información, sino también para asesorarlos en el llenado de las mismas.

Es hasta la emisión de la ahora vigente Ley Federal de Transparencia y Acceso a la Información Pública del 9 de mayo de 2016, en donde se cambia de Unidad de Enlace a Unidad de Transparencia y se crean nuevas funciones para que la Unidad sea una promotora de las políticas de transparencia proactiva y para que fomente la transparencia dentro del sujeto obligado. Su tarea también consiste en comunicar, dentro de la institución correspondiente, la trascendencia de cumplir con el derecho de acceso a la información pública de los solicitantes y de la obligación constitucional de aplicar el principio de máxima publicidad. Además, se convierte en la instancia que hace del conocimiento a las autoridades competentes de la probable responsabilidad en el caso en el que los funcionarios no cumplan en tiempo y forma con las solicitudes de acceso.

## II. Relevancia temática y contexto

La relevancia de la Unidad de Transparencia consiste en ser el primer contacto del sujeto obligado con el particular para garantizar la tutela de dos derechos humanos consagrados en el artículo 6º y en el artículo 19 de la Constitución Política de los Estados Unidos Mexicanos: el derecho de acceso a la información y el derecho a la protección de datos personales. En este sentido, su conocimiento y sensibilización en datos personales, así como su actuar para procurar condiciones de igualdad para garantizar este derecho a grupos vulnerables o personas con discapacidad, son fundamentales en una sociedad democrática que aspira a tener igualdad en el ejercicio de los derechos humanos.

La Unidad de Transparencia garantiza y es responsable de la gestión de las solicitudes del ejercicio de los derechos ARCO, por lo que su función es muy relevante ya que es la que da viabilidad al ejercicio y tutela del derecho a la protección de datos personales.

## III. Análisis del contenido

El artículo 85 de esta ley general nos remite al Capítulo IV De las Unidades de Transparencia, artículos 45 y 46 de la LGTAIP, en los cuales se establecen las funciones de la Unidad para establecer el procedimiento y los trámites para dar contestación a las solicitudes de acceso a la información.[208]

[208] "Artículo 45. Los sujetos obligados designarán al responsable de la Unidad de Transparencia que tendrá las siguientes funciones:
I. Recabar y difundir la información a que se refieren los Capítulos II, III, IV y V del Título Quinto de esta Ley, así como la correspondiente de la Ley Federal y de las Entidades Federativas y propiciar que las Áreas la actualicen periódicamente, conforme la normatividad aplicable;
II. Recibir y dar trámite a las solicitudes de acceso a la información;
III. Auxiliar a los particulares en la elaboración de solicitudes de acceso a la información y, en su caso, orientarlos sobre los sujetos obligados competentes conforme a la normatividad aplicable;
IV. Realizar los trámites internos necesarios para la atención de las solicitudes de acceso a la información;
V. Efectuar las notificaciones a los solicitantes;

Respecto al derecho a la protección de datos personales, la LGPDPPSO dispone que la Unidad de Transparencia sea la encargada de ayudar y orientar en el ejercicio de este derecho. Las funciones de la Unidad de Transparencia son fundamentales y necesarias para tutelar el derecho a la protección de datos personales, ya que es la primera en tener contacto con las solicitudes de acceso, rectificación, cancelación y oposición de los datos personales, pues una de sus principales funciones, de conformidad con lo dispuesto en la fracción II, es gestionar las solicitudes para el ejercicio de los derechos ARCO, así como la contemplada en la fracción V, de proponer al Comité de Transparencia los procedimientos internos que aseguren y fortalezcan mayor eficiencia en la gestión de las solicitudes para el ejercicio de los derechos ARCO. También son funciones importantes de la Unidad de Transparencia asesorar al responsable de las áreas adscritas, en materia de protección de datos personales, ya que estas áreas generan la información y deben saber sus obligaciones en cuanto al tratamiento de los datos.

Debido a que el encargado de la Unidad de Transparencia es el primer contacto con la tutela de este derecho y asesora a las áreas en la protección de datos personales, es fundamental que tenga un amplio conocimiento sobre esta materia. Adicionalmente, la función que tiene de orientar y auxiliar en el manejo de datos personales y asesorar a las distintas áreas de las instituciones sobre esta materia es fundamental para poder hacer efectivo este derecho y garantizar su cabal cumplimiento.

Una figura que se establece en esta ley es la del oficial de protección de datos personales. Esta figura si bien no es obligatoria, es de suma importancia ya que funge como asesor especialista en datos personales para la gestión en el tratamiento de los datos, la adopción de medidas de seguridad, la atención de los derechos ARCO, etc.

---

VI. Proponer al Comité de Transparencia los procedimientos internos que aseguren la mayor eficiencia en la gestión de las solicitudes de acceso a la información, conforme a la normatividad aplicable;
VII. Proponer personal habilitado que sea necesario para recibir y dar trámite a las solicitudes de acceso a la información;
VIII. Llevar un registro de las solicitudes de acceso a la información, respuestas, resultados, costos de reproducción y envío;
IX. Promover e implementar políticas de transparencia proactiva procurando su accesibilidad;
X. Fomentar la transparencia y accesibilidad al interior del sujeto obligado;
XI. Hacer del conocimiento de la instancia competente la probable responsabilidad por el incumplimiento de las obligaciones previstas en la presente Ley y en las demás disposiciones aplicables, y
XII. Las demás que se desprendan de la normatividad aplicable.
Los sujetos obligados promoverán acuerdos con instituciones públicas especializadas que pudieran auxiliarles a entregar las repuestas a solicitudes de información, en la lengua indígena, braille o cualquier formato accesible correspondiente, en forma más eficiente.
Artículo 46. Cuando alguna Área de los sujetos obligados se negara a colaborar con la Unidad de Transparencia, ésta dará aviso al superior jerárquico para que le ordene realizar sin demora las acciones conducentes.
Cuando persista la negativa de colaboración, la Unidad de Transparencia lo hará del conocimiento de la autoridad competente para que ésta inicie, en su caso, el procedimiento de responsabilidad respectivo".

Por su parte, el artículo 86 marca un objetivo de inclusión relevante y de vanguardia en la protección de este derecho, ya que establece que el responsable debe procurar la protección de los datos personales para aquellos grupos vulnerables o con algún tipo de discapacidad. La redacción de este artículo nos lleva a interpretar que el responsable de datos procurará garantizar el ejercicio de este derecho, es decir, hará su mayor esfuerzo para ello. Sin embargo, no se establece como un mandato obligatorio, lo que puede dejar a las personas con discapacidad o grupos vulnerables en estado de indefensión y sin la protección de sus datos personales contraviniendo los artículos 1º y 16º constitucionales.

Finalmente, el artículo 87 nos remite a LGTAIP la cual en el artículo 45 señala que los sujetos obligados designarán al responsable de la Unidad de Transparencia y señala las funciones que debe desempañar. Una de las actividades más significativas de la Unidad de Transparencia es la de recibir y dar trámite a las solicitudes de acceso a la información. Como es el primer contacto del sujeto obligado con la sociedad, agiliza la búsqueda de la información, promueve la transparencia proactiva, entre otras funciones. Además, es un coadyuvante entre el sujeto obligado y el ciudadano pues promueve, en todo momento, la búsqueda y entrega de la información.

## IV. Conclusiones

De lo anterior, podemos concluir que tanto la Unidad de Transparencia como el Comité, son las figuras más relevantes en la realización y cumplimiento de los derechos ARCO de los particulares, pues a pesar de que no son las áreas que hacen algún tipo de tratamiento de datos, ni las poseedoras de la información, sí son las que reciben, dan seguimiento, atienden y resuelven las solicitudes relativas a este derecho. Asimismo, son los encargados de testar la información para generar versiones públicas y de clasificar la información en caso de que proceda salvaguardar el derecho a la protección de datos personales. La Unidad de Transparencia debe alertar e identificar la existencia de datos personales y de datos personales sensibles y notificar a las áreas de los sujetos obligados si ya venció el tiempo para desclasificar la información reservada, por lo que resulta indispensable que los integrantes de la Unidad tengan experiencia y se capaciten en esta materia.

La Unidad de Transparencia también se convierte en la oficina que está en constante contacto con las áreas que ostentan la información y, en la práctica, una de sus funciones ha sido la de sensibilizar a los sujetos obligados para que den cumplimiento a la información solicitada. También fungen como área de apoyo para identificar y proteger los datos personales, por lo que la profesionalización del personal de la Unidad debe ser fundamental, ya que son el vínculo que garantiza el derecho de acceso a la información y el derecho a la protección de datos personales.

Finalmente, la función que tiene de orientar y auxiliar en el manejo de datos personales y asesorar a las distintas áreas, obliga a que el perfil del titular del área y el personal de apoyo sean especialistas en datos personales y puedan garantizar y hacer efectivo este derecho con el objetivo de asegurar su cabal cumplimiento. Asimismo, la Unidad de Transparencia al ser gestora y asesora directa de los particulares también se convierte en promotora e interlocutora entre la autoridad y la ciudadanía, procurando agilizar los procesos internos para dar respuesta oportuna a los particulares.

## Referencias

Cámara de Diputados. (2002). *Dictamen de la Comisión de Gobernación y Seguridad Pública, con proyecto de Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Proyecto de Decreto de Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*.

DOF. (2014). Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, *Diario Oficial de la Federación*.

DOF. (2015). Ley General de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*.

DOF. (2016). Ley Federal de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*.

# TÍTULO OCTAVO
# ORGANISMOS GARANTES

# CAPÍTULO I
# DEL INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES

***Artículo 88.*** *En la integración, procedimiento de designación y funcionamiento del Instituto y del Consejo Consultivo se estará a lo dispuesto por la Ley General de Transparencia y Acceso a la Información Pública, la Ley Federal de Transparencia y Acceso a la Información Pública y demás normativa aplicable.*

***Artículo 89.*** *Además de las facultades que le son conferidas en la Ley General de Transparencia y Acceso a la Información Pública, la Ley Federal de Transparencia y Acceso a la Información Pública y demás normatividad que le resulte aplicable, el Instituto tendrá las siguientes atribuciones:*

*I. Garantizar el ejercicio del derecho a la protección de datos personales en posesión de sujetos obligados;*

*II. Interpretar la presente Ley en el ámbito administrativo;*

*III. Conocer y resolver los recursos de revisión que interpongan los titulares, en términos de lo dispuesto en la presente Ley y demás disposiciones que resulten aplicables en la materia;*

*IV. Conocer y resolver, de oficio o a petición fundada por los organismos garantes, los recursos de revisión que por su interés y trascendencia así lo ameriten, en términos de lo dispuesto en la presente Ley y demás disposiciones que resulten aplicables en la materia;*

*V. Conocer y resolver los recursos de inconformidad que interpongan los titulares, en contra de las resoluciones emitidas por los organismos garantes, de conformidad con lo dispuesto en la presente Ley y demás disposiciones que resulten aplicables en la materia;*

*VI. Conocer, sustanciar y resolver los procedimientos de verificación;*

*VII. Establecer y ejecutar las medidas de apremio previstas en términos de lo dispuesto por la presente Ley y demás disposiciones que resulten aplicables en la materia;*

*VIII. Denunciar ante las autoridades competentes las presuntas infracciones a la presente Ley y, en su caso, aportar las pruebas con las que cuente;*

*IX. Coordinarse con las autoridades competentes para que las solicitudes para el ejercicio de los derechos ARCO y los recursos de revisión que se presenten en lengua indígena, sean atendidos en la misma lengua;*

*X. Garantizar, en el ámbito de su respectiva competencia, condiciones de accesibilidad para que los titulares que pertenecen a grupos vulnerables puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales;*

*XI. Elaborar y publicar estudios e investigaciones para difundir y ampliar el conocimiento sobre la materia de la presente Ley;*

*XII. Proporcionar apoyo técnico a los responsables para el cumplimiento de las obligaciones establecidas en la presente Ley;*

*XIII. Divulgar y emitir recomendaciones, estándares y mejores prácticas en las materias reguladas por la presente Ley;*

*XIV. Vigilar y verificar el cumplimiento de las disposiciones contenidas en la presente Ley;*

*XV. Administrar el registro de esquemas de mejores prácticas a que se refiere la presente Ley y emitir sus reglas de operación;*

*XVI. Emitir, en su caso, las recomendaciones no vinculantes correspondientes a la Evaluación de impacto en la protección de datos personales que le sean presentadas;*

*XVII. Emitir disposiciones generales para el desarrollo del procedimiento de verificación;*

*XVIII. Realizar las evaluaciones correspondientes a los esquemas de mejores prácticas que les sean notificados, a fin de resolver sobre la procedencia de su reconocimiento o validación e inscripción en el registro de esquemas de mejores prácticas, así como promover la adopción de los mismos;*

*XIX. Emitir, en el ámbito de su competencia, las disposiciones administrativas de carácter general para el debido cumplimiento de los principios, deberes y obligaciones que establece la presente Ley, así como para el ejercicio de los derechos de los titulares;*

*XX. Celebrar convenios con los responsables para desarrollar programas que tengan por objeto homologar tratamientos de datos personales en sectores específicos, elevar la protección de los datos personales y realizar cualquier mejora a las prácticas en la materia;*

*XXI. Definir y desarrollar el sistema de certificación en materia de protección de datos personales, de conformidad con lo que se establezca en los parámetros a que se refiere la presente Ley;*

*XXII. Presidir el Sistema Nacional a que se refiere el artículo 10 de la presente Ley;*

*XXIII. Celebrar convenios con los organismos garantes que coadyuven al cumplimiento de los objetivos previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia;*

*XXIV. Llevar a cabo acciones y actividades que promuevan el conocimiento del derecho a la protección de datos personales, así como de sus prerrogativas;*

*XXV. Diseñar y aplicar indicadores y criterios para evaluar el desempeño de los responsables respecto al cumplimiento de la presente Ley y demás disposiciones que resulten aplicables en la materia;*

*XXVI. Promover la capacitación y actualización en materia de protección de datos personales entre los responsables;*

*XXVII. Emitir lineamientos generales para el debido tratamiento de los datos personales;*

*XXVIII. Emitir lineamientos para homologar el ejercicio de los derechos ARCO;*

*XXIX. Emitir criterios generales de interpretación para garantizar el derecho a la protección de datos personales;*

*XXX. Cooperar con otras autoridades de supervisión y organismos nacionales e internacionales, a efecto de coadyuvar en materia de protección de datos personales, de conformidad con las disposiciones previstas en la presente Ley y demás normativa aplicable;*

*XXXI. Promover e impulsar el ejercicio y tutela del derecho a la protección de datos personales a través de la implementación y administración de la Plataforma Nacional, a que se refiere la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable;*

*XXXII. Interponer, cuando así lo aprueben la mayoría de sus Comisionados, acciones de inconstitucionalidad en contra de leyes de carácter federal o estatal, así como de los Tratados Internacionales celebrados por el Ejecutivo Federal y aprobados por el Senado de la República, que vulneren el derecho a la protección de datos personales;*

*XXXIII. Promover, cuando así lo aprueben la mayoría de sus Comisionados, las controversias constitucionales en términos del artículo 105, fracción I, inciso l), de la Constitución Política de los Estados Unidos Mexicanos;*

*XXXIV. Cooperar con otras autoridades nacionales o internacionales para combatir conductas relacionadas con el indebido tratamiento de datos personales;*

*XXXV. Diseñar, vigilar y, en su caso, operar el sistema de buenas prácticas en materia de protección de datos personales, así como el sistema de certificación en la materia, a través de normativa que el Instituto emita para tales fines;*

*XXXVI. Celebrar convenios con los organismos garantes y responsables que coadyuven al cumplimiento de los objetivos previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia, y*

*XXXVII. Las demás que le confiera la presente Ley y demás ordenamientos aplicables.*

## COMENTARIO

**Jimena Moreno González**

### I. Antecedentes

En la abrogada LFTAIPG de 2002 y a través de Decreto presidencial publicado en el *Diario Oficial de la Federación* el 24 de diciembre de 2002, se crea el Instituto Federal de Acceso a la Información Pública, como "un organismo descentralizado, no sectorizado, con personalidad jurídica y patrimonio propio, con domicilio legal en la Ciudad de México". De igual forma, el decreto de creación del Instituto establece que el mismo cuenta "con autonomía operativa, presupuestaria y de decisión […]". (artículo 1).

En su conformación original, el Instituto estaba integrado por cinco comisionados, su encargo era por siete años sin posibilidad de reelección, eran nombrados por el Ejecutivo Federal y podrían ser objetados por la mayoría de la Cámara de Senadores. "La discusión en la creación de este órgano radicó principalmente en la necesidad de establecer una institución encargada de garantizar el derecho de acceso a la información y la transparencia en la actividad pública gubernamental, para el fortalecimiento de las instituciones en general".[209]

[209] Kurczyn, P. (2015). La Autonomía Constitucional del Órgano Garante de Transparencia, Acceso a la Información y Protección de Datos Personales, *Revista de Administración Pública*, vol. L, núm. 3, septiembre-diciembre, p. 143.

Se dotó de autonomía operativa, presupuestaria y de decisión al Instituto, con el objeto de que tuviera mayor independencia respecto a otras dependencias de la Administración Pública Federal. Se le dio la facultad de resolver la negativa a las solicitudes de acceso a la información y de datos personales, así como de determinar la clasificación a información reservada o confidencial. Sus principales funciones eran la de garantizar y promover el derecho de acceso a la información y el derecho a la protección de datos personales en poder de las dependencias.

La LFPDPPP, publicada en el *Diario Oficial de la Federación* el 7 de julio de 2010, señala al Instituto Federal de Acceso a la Información Pública como la autoridad competente en el derecho a la protección de datos personales en posesión de particulares y, por ende, cambia de nombre originario a Instituto Federal de Acceso a la Información y Protección de Datos (IFAI, ahora INAI). En esta ley se regula el tratamiento de datos personales en posesión de los particulares, y el Instituto es el garante de la privacidad y del derecho a la autodeterminación informativa de las personas.

En la reforma al artículo 6º constitucional del 7 de febrero de 2014 se cambia la naturaleza jurídica al Instituto para otorgarle autonomía constitucional, lo que significa no depender de ninguno de los tres poderes y tener autonomía técnica, de gestión y presupuestaria, con patrimonio propio y personalidad jurídica.[210] Así se fortalece al Instituto y se le dota de independencia, se le dan mayores competencias y funciones para garantizar el acceso a información y el derecho a la protección de datos personales.

[210] ÓRGANOS CONSTITUCIONALES AUTÓNOMOS. NOTAS DISTINTIVAS Y CARACTERÍSTICAS. El Tribunal en Pleno de la Suprema Corte de Justicia de la Nación respecto de los órganos constitucionales autónomos ha sostenido que: 1. Surgen bajo una idea de equilibrio constitucional basada en los controles de poder, evolucionando así la teoría tradicional de la división de poderes dejándose de concebir la organización del Estado derivada de los tres tradicionales (Ejecutivo, Legislativo y Judicial) que, sin perder su esencia, debe considerarse como una distribución de funciones o competencias, haciendo más eficaz el desarrollo de las actividades encomendadas al Estado. 2. Se establecieron en los textos constitucionales, dotándolos de garantías de actuación e independencia en su estructura orgánica para que alcancen los fines para los que fueron creados, es decir, para que ejerzan una función propia del Estado que por su especialización e importancia social requería autonomía de los clásicos poderes del Estado. 3. La creación de este tipo de órganos no altera o destruye la teoría tradicional de la división de poderes, pues la circunstancia de que los referidos órganos guarden autonomía e independencia de los poderes primarios, no significa que no formen parte del Estado mexicano, pues su misión principal radica en atender necesidades torales tanto del Estado como de la sociedad en general, conformándose como nuevos organismos que se encuentran a la par de los órganos tradicionales. Atento a lo anterior, las características esenciales de los órganos constitucionales autónomos son: a) Deben estar establecidos directamente por la Constitución Federal; b) Deben mantener, con los otros órganos del Estado, relaciones de coordinación; c) Deben contar con autonomía e independencia funcional y financiera; y d) Deben atender funciones primarias u originarias del Estado que requieran ser eficazmente atendidas en beneficio de la sociedad. Suprema Corte de Justicia de la Nación. (mayo de 2007). Tesis Jurisprudencial P./J. 20/2007. Novena Época, *Semanario Judicial de la Federación y su Gaceta*, Tomo XXV, p. 1647.

El artículo 6º de la CPEUM señala las bases del ejercicio del derecho de acceso a la información y de la protección de datos personales y en la fracción VIII se otorga al INAI autonomía constitucional en los términos siguientes:

> La Federación contará con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley.

"Uno de los temas centrales de la discusión respecto de los órganos reguladores es la idea de 'independencia' o 'autonomía'. Ésta se refiere principalmente al aislamiento formal e informal de estos órganos de las presiones de grupos de interés políticos, burocráticos o sociales, y que llevaría a 'mejorar la transparencia, estabilidad y capacidad técnica' (OCDE,2002, 95)".[211]

En cumplimiento a esta reforma se expidió la Ley General de Transparencia y Acceso a la Información Pública publicada en el *Diario Oficial de la Federación* el 4 de mayo del 2015 y se vuelve a cambiar de denominación para ser el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos (INAI). Sus resoluciones son vinculatorias, definitivas e inatacables salvo en el caso que dichas resoluciones puedan poner en peligro la seguridad nacional conforme a la ley de la materia. En este caso, el Consejero Jurídico del Gobierno podrá interponer recurso de revisión ante la Suprema Corte de Justicia de la Nación.

## II. Relevancia temática y contexto

En una sociedad democrática contar con un organismo autónomo e imparcial que vele y garantice la protección de datos personales de las personas físicas frente a los órganos del Estado pero también frente a los particulares, es esencial. El diseño institucional y las facultades de revisión y atracción conferidas al INAI hacen del Instituto un auténtico garante de los derechos. Sus resoluciones van definiendo la interpretación y el alcance de este derecho y van sentando precedentes que ayudan a garantizar su protección.

En una sociedad en la que la información personal en posesión de los sujetos obligados y de los particulares contiene datos personales y datos personales sensibles y el uso de éstos puede poner a las personas en

[211] López Ayllón, S. y Haddou, A. (2007). Rendición de cuentas y diseño institucional de los órganos reguladores en México, *Gestión y Política Pública*, Centro de Investigación y Docencia Económicas (CIDE), vol. XVI, núm. 1, p. 113.

situaciones de riesgo o de discriminación y además tienen un valor en el mercado, el derecho a la protección de datos personales se convierte en una necesidad, por lo que garantizar su protección, hacer efectivo este derecho, velar por la privacidad y la seguridad de la información, a fin de evitar abusos, son parte de los grandes retos del INAI.

## III. Análisis del contenido

El INAI como órgano garante es responsable de tutelar el derecho de protección de datos personales en posesión de sujetos obligados y a raíz de la reforma constitucional al artículo 6º y de la expedición de la Ley General de Protección de Datos Personales se le otorgaron amplias facultades en la materia.

Como se desprende de las diversas fracciones del artículo 89, el INAI cuenta con atribuciones para realizar procedimientos de verificación (fracción VI); para conocer y resolver los recursos de revisión (fracción III); así como "los recursos que interpongan los particulares respecto de las resoluciones de los organismos autónomos especializados de las entidades federativas que determinen la reserva, confidencialidad, inexistencia o negativa de la información, en los términos que establezca la ley".[212] Este último corresponde, en términos de la LGPDPPSO, al llamado recurso de inconformidad que se interpone en contra de las resoluciones de los órganos garantes estatales (fracción V). La facultad que tiene el INAI para conocer y resolver asuntos de los estados contribuye a tener una visión general y uniforme en la interpretación de este derecho.

Asimismo, se le otorga la facultad de atracción para conocer y resolver, de oficio o a petición de parte, de los recursos de revisión que por su interés y trascendencia así lo ameriten (fracción IV). Aún y cuando el INAI ha establecido lineamientos generales de interpretación,[213] es importante mencionar que esta facultad contempla un margen de discrecionalidad para atraer casos, por lo que es fundamental que la ejerza de manera congruente y precisa, a fin de evitar la arbitrariedad.

Una de las atribuciones más relevantes es la facultad que tiene el INAI para imponer medidas de apremio y denunciar presuntas infracciones a la ley (fracciones VII y VII). A través de estas facultades se garantiza el derecho a la protección de datos personales en caso de que los sujetos obligados no cumplan con las resoluciones del órgano garante, o bien, infrinjan las disposiciones de la ley.

[212] Véase el artículo 6º, apartado A, fracción VIII, párr. cuarto, de la CPEUM.

[213] Véase el "Acuerdo mediante el cual se aprueban los nuevos Lineamientos generales para que el INAI ejerza la facultad de atracción", emitidos por el INAI y publicados en el *Diario Oficial de la Federación* el 16 de febrero de 2017.

La facultad de interponer acciones de inconstitucionalidad en contra de leyes de carácter federal o estatal o de tratados internacionales que vulneren el derecho a la protección de datos personales (fracción XXXII), así como la facultad para promover controversias constitucionales (fracción XXXIII), fortalece al INAI como un verdadero organismo autónomo que no sólo es garante de este derecho sino que es un jugador en el equilibrio de poderes ya que lo lleva a guardar y velar por la regularidad constitucional.

El INAI también tiene la función de fomentar una cultura de protección de datos personales a través de la realización de diversas actividades o la elaboración o publicación de estudios e investigaciones que difundan su conocimiento (fracciones XXIV y XI), así como mediante el apoyo técnico y la promoción de la capacitación y actualización de los responsables del tratamiento de datos personales (fracciones XII y XXVI). Estas funciones son esenciales para poder acercarse tanto a los ciudadanos como a los responsables del tratamiento de datos personales, a fin de dar a conocer la importancia de proteger la información personal y de los mecanismos existentes, sea para ejercer un derecho o para cumplir con las obligaciones respectivas.

Asimismo, el INAI debe asegurarse de garantizar condiciones de igualdad en grupos vulnerables e indígenas para que no sólo gocen de la protección efectiva de sus datos personales, sino que también puedan ejercitar sus derechos. Ello supone la adopción de medidas que garanticen su accesibilidad (fracciones IX y X).

El Instituto cuenta con diversas facultades regulatorias que le permiten emitir, en el marco de sus facultades, lineamientos y disposiciones administrativas con alcance general, que coadyuvan a la certidumbre jurídica. Al respecto, el INAI está facultado para: 1) Emitir disposiciones generales sobre el desarrollo del procedimiento de verificación (fracción XVII); 2) Emitir disposiciones administrativas de carácter general para el debido cumplimiento del contenido de esta ley, relativo a los principios, deberes y obligaciones, así como para el ejercicio de los derechos por parte de los titulares de los datos personales (fracción XIX); 3) Emitir lineamientos generales para el debido tratamiento de datos personales (fracción XXVII), y 4) Emitir lineamientos con el objeto de homologar el ejercicio de los derechos ARCO (fracción XXVIII). De igual forma, en un sentido similar a la conformación de precedentes jurisprudenciales, el INAI está facultado para emitir criterios generales de interpretación para garantizar el derecho a la protección de datos personales (fracción XXIX).

En cuanto a la emisión de lineamientos en el tratamiento de datos personales, éstos deberán incluir 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.[214] La emisión de lineamientos en el tratamiento de datos personales es un reto para el INAI, ya que incluye todo el proceso manual y automatizado, desde la obtención de los datos personales hasta su transferencia y, en el caso de datos personales sensibles, deberá, además, generar lineamientos con estándares de protección más amplios.

Ahora bien, por lo que hace al Consejo Consultivo del INAI al que se refiere el artículo 88 de esta ley, cabe decir que las bases para su funcionamiento están previstas en la LGTAIP (artículos 47 y 48) y en la LFTAIP (artículos 53 al 60). De conformidad con estos ordenamientos, en congruencia con lo dispuesto por el artículo 6º de la CPEUM, este órgano constitucional ciudadano debe estar integrado por diez consejeros honoríficos aprobados (previa consulta con la sociedad) por las dos terceras partes de los miembros del Senado de la República y durarán como máximo siete años en su cargo. En la integración del Consejo se debe garantizar la igualdad de género y sus integrantes deberán ser especialistas en la materia de transparencia, acceso a la información, datos personales y en derechos humanos. Además, deberán ser integrantes de la sociedad civil y la academia.

La función principal del Consejo es la de emitir opiniones no vinculantes sobre transparencia, acceso a la información, accesibilidad y protección de datos personales. También deberá pronunciarse sobre el desempeño del INAI, su informe anual, presupuesto, funcionamiento, plan de trabajo, entre otras opiniones, las cuales deberán ser públicas.

Además de ser un órgano que acompaña al Instituto respecto a su desempeño institucional como garante de los artículos 6º y 16 constitucional, emite opiniones y hace sugerencias sobre estos temas, también es un vínculo y promotor cercano a la ciudadanía en los proyectos y acciones, regulación y evaluación en materia de datos abiertos.

El Consejo Consultivo del INAI nace de la necesidad de tener un diálogo abierto y constante con la sociedad en estos temas, el cual deberá establecer las bases para interactuar con los diferentes sectores de la sociedad civil y la academia. Es un representante con voz pública, integrado por especialistas en estas materias y cuyas opiniones son recomendaciones que deberá atender el Instituto, aun cuando no las adopte.

[214] Cfr. Artículo 3, fracción XXXIII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

## IV. Conclusiones

A lo largo de las diversas reformas constitucionales se ha venido definiendo al INAI como una institución con facultades y funciones que le permitan ser un verdadero garante del derecho de acceso a la información y del derecho a la protección de datos personales, con facultades para intervenir, de manera específica, en las decisiones trascendentes de los órganos garantes locales y con autonomía técnica, para que pueda interpretar y aplicar la normatividad de manera que disminuya el rango de discrecionalidad y cubra los vacíos legales que se puedan generar.

En una sociedad donde la tecnología pone en riesgo la privacidad y el uso y abuso de los datos personales son cada vez mayores, los desafíos que enfrenta el INAI en salvaguardar este derecho son complejos no sólo por los avances tecnológicos en el uso de información personal sino porque también tiene la encomienda de generar una cultura de protección de los datos personales en una sociedad donde la privacidad se disminuye de forma acelerada.

## Referencias

DOF. (2014). Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, *Diario Oficial de la Federación*. [Archivo PDF]. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_215_07feb14.pdf, [fecha de consulta: 8 de mayo 2018).

DOF. (2015). Ley General de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*.

DOF. (2016). Ley Federal de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación.*

Kurczyn, P. (2015). La Autonomía Constitucional del Órgano Garante de Transparencia, Acceso a la Información y Protección de Datos Personales, *Revista de Administración Pública*, vol. L, núm. 3, septiembre-diciembre, pp. 139-154.

López Ayllón, S. y Haddou, A. (2007). *Rendición de cuentas y diseño institucional de los órganos reguladores en México, Gestión y Política Pública*, Centro de Investigación y Docencia Económicas (CIDE), vol. XVI, núm. 1, pp. 101-145.

Suprema Corte de Justicia de la Nación. (mayo de 2007). Tesis Jurisprudencial P./J. 20/2007. Novena Época, *Semanario Judicial de la Federación y su Gaceta*, Tomo XXV, p. 1647.

# CAPÍTULO II
# DE LOS ORGANISMOS GARANTES

***Artículo 90.*** *En la integración, procedimiento de designación y funcionamiento de los organismos garantes se estará a lo dispuesto por la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable.*

***Artículo 91.*** *Para los efectos de la presente Ley y sin perjuicio de otras atribuciones que les sean conferidas en la normatividad que les resulte aplicable, los organismos garantes tendrán las siguientes atribuciones:*

*I. Conocer, sustanciar y resolver, en el ámbito de sus respectivas competencias, de los recursos de revisión interpuestos por los titulares, en términos de lo dispuesto en la presente Ley y demás disposiciones que resulten aplicables en la materia;*

*II. Presentar petición fundada al Instituto, para que conozca de los recursos de revisión que por su interés y trascendencia así lo ameriten, en términos de lo previsto en la presente Ley y demás disposiciones que resulten aplicables en la materia;*

*III. Imponer las medidas de apremio para asegurar el cumplimiento de sus resoluciones;*

*IV. Promover y difundir el ejercicio del derecho a la protección de datos personales;*

*V. Coordinarse con las autoridades competentes para que las solicitudes para el ejercicio de los derechos ARCO y los recursos de revisión que se presenten en lenguas indígenas, sean atendidos en la misma lengua;*

*VI. Garantizar, en el ámbito de sus respectivas competencias, condiciones de accesibilidad para que los titulares que pertenecen a grupos vulnerables puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales;*

*VII. Elaborar y publicar estudios e investigaciones para difundir y ampliar el conocimiento sobre la materia de la presente Ley;*

*VIII. Hacer del conocimiento de las autoridades competentes, la probable responsabilidad derivada del incumplimiento de las obligaciones previstas en la presente Ley y en las demás disposiciones que resulten aplicables;*

*IX. Proporcionar al Instituto los elementos que requiera para resolver los recursos de inconformidad que le sean presentados, en términos de lo previsto en el Título Noveno, Capítulo II de la presente Ley y demás disposiciones que resulten aplicables en la materia;*

*X. Suscribir convenios de colaboración con el Instituto para el cumplimiento de los objetivos previstos en la presente Ley y demás disposiciones aplicables;*

*XI. Vigilar, en el ámbito de sus respectivas competencias, el cumplimiento de la presente Ley y demás disposiciones que resulten aplicables en la materia;*

*XII. Llevar a cabo acciones y actividades que promuevan el conocimiento del derecho a la protección de datos personales, así como de sus prerrogativas;*

*XIII. Aplicar indicadores y criterios para evaluar el desempeño de los responsables respecto del cumplimiento de la presente Ley y demás disposiciones que resulten aplicables;*

*XIV. Promover la capacitación y actualización en materia de protección de datos personales entre los responsables;*

*XV. Solicitar la cooperación del Instituto en los términos del artículo 89, fracción XXX de la presente Ley;*

*XVI. Administrar, en el ámbito de sus competencias, la Plataforma Nacional de Transparencia;*

*XVII. Según corresponda, interponer acciones de inconstitucionalidad en contra de leyes expedidas por las legislaturas de las Entidades Federativas, que vulneren el derecho a la protección de datos personales, y*

*XVIII. Emitir, en su caso, las recomendaciones no vinculantes correspondientes a la Evaluación de impacto en protección de datos personales que le sean presentadas.*

# COMENTARIO

**Gisela María Pérez Fuentes**

## I. Antecedentes

Es una obligación del Estado recurrir al diseño de formas de protección adecuadas que tutelen el derecho a la protección de datos personales. Lo anterior se puede lograr por medio de mecanismos genéricos (aplicables a todos los derechos) y específicos (aplicables a la protección de los datos personales).[215]

Según las pautas impuestas por la Corte Interamericana de Derechos Humanos, pueden establecerse los siguientes tipos de garantía:

a) De aseguramiento. En el caso de México, el mecanismo establecido para la protección de datos personales en posesión de sujetos obligados, se encuentra reconocido de forma vigente en su nueva ley en la materia, es decir, la LGPDPPSO que se publicó en el DOF el 26 de enero de 2017.

b) Jurisdiccional. Mediante el establecimiento del recurso de revisión la LGPDPPSO prevé la tutela efectiva ante la inconformidad de la solicitud para el ejercicio de los derechos ARCO. La ley mexicana de la materia establece un plazo que no podrá exceder de cuarenta días y que, por una única ocasión, podrá ampliarse hasta por veinte días.

c) Reparadoras. Todo el que cometa un daño a otro está obligado a repararlo, en el caso de la protección de datos personales, la LGPDPPSO considera que las responsabilidades que resulten de los procedimientos administrativos correspondientes, derivados de la violación al derecho fundamental de la protección de datos personales, son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos (artículo 165).

d) Punitivas. El derecho a la protección de datos personales prevé, en su ley general, la imposición de medidas de apremio para que los organismos garantes aseguren el cumplimiento de sus resoluciones. En el caso de México, los órganos garantes no son los que establecen las sanciones para los sujetos obligados de la administración pública, sino que una vez detectada la presunta responsabilidad administrativa, deben remitir una denuncia dirigida a la contraloría, órgano interno de control o equivalente, con la descripción precisa de los actos u omisiones que, a su consideración, repercuten en la adecuada aplicación de la ley y que pudieran constituir una posible responsabilidad.

[215] Puccinelli, O. (2004). P*rotección de datos de carácter personal.* Buenos Aires: Ed. Astrea.

## II. Relevancia temática y contexto

En el derecho comparado los organismos garantes en materia de protección de datos personales se organizan conforme a la legislación interna de cada país, por ejemplo, Alemania tiene un organismo federal y varios regionales (a través de sus estados federados llamados *Länder*) que cuentan con leyes propias de protección de datos. Francia cuenta con una comisión compuesta por más de diez miembros y con algunas competencias similares a la figura del ombudsman. Gran Bretaña, por su parte, posee instituciones como el *data protector* y un tribunal especializado en la tutela de los derechos cívicos frente a eventuales abusos informáticos. En España existe la Agencia Nacional de Protección de Datos, así como las agencias organizadas por las comunidades autónomas.[216]

La experiencia europea demostró que es útil contar con un sistema protector y con organismos garantes, ya que la tendencia en la materia establece la necesidad de regular las facultades y atribuciones de tales organismos.

En México, el INAI, es el organismo garante de la Federación en materia de protección de datos personales en posesión de los sujetos obligados.

La protección de datos personales y el derecho de acceso a la información se han convertido en derechos fundamentales amparados por la CPEUM a través de sus órganos garantes. Los principios a los que se hace referencia aparecen en el artículo 6º constitucional en el siguiente apartado:

> A. Para el ejercicio del derecho de acceso a la información, la Federación y las entidades federativas, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:
>
> [...]
>
> VIII. La Federación contará con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley.
>
> El organismo autónomo previsto en esta fracción se regirá por la ley en materia de transparencia y acceso a la información pública y protección

[216] *Idem.*

> de datos personales en posesión de sujetos obligados, en los términos que establezca la ley general que emita el Congreso de la Unión para establecer las bases, principios generales y procedimientos del ejercicio de este derecho.

Para el posible desarrollo del órgano autónomo, la propia Constitución define la facultad o función del órgano garante que desarrollará la vigilancia y control tanto de la transparencia como en forma ponderada sobre la protección de los datos personales.

Otro de los principios que marca la Constitución de México es que el organismo garante tiene competencia para conocer los asuntos relacionados con el acceso a la información pública y la protección de datos personales de cualquier autoridad, entidad, órgano u organismo que forme parte de alguno de los poderes (Legislativo, Ejecutivo y Judicial), órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicatos que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, con excepción de aquellos asuntos jurisdiccionales que correspondan a la Suprema Corte de Justicia de la Nación, en cuyo caso resolverá un comité integrado por tres ministros.

El órgano garante a nivel nacional puede conocer, también, los recursos que interpongan los particulares respecto de las resoluciones de los organismos autónomos especializados de las entidades federativas que determinen la reserva, confidencialidad, inexistencia o negativa de la información, en los términos que establezca la ley.

Otra de las bases que se incorporó en la Constitución en la reforma de 2016, para la protección de datos personales, fue que el organismo garante federal, de oficio o a petición fundada del organismo garante equivalente de las entidades federativas, podrá conocer los recursos de revisión que por su interés y trascendencia así lo ameriten, es decir, tendrá la facultad de atracción de casos relevantes que ocurran en los estados del país.

La LGPDPPSO, reglamentaria de la Constitución, ratifica la definición de los órganos garantes al considerarlos organismos con autonomía constitucional y especializados en materia de acceso a la información y protección de datos personales. De igual forma, se establecen los dos tipos de órganos garantes existentes: el federal y los estatales. Estos últimos (a los cuales corresponde el presente análisis) están amparados en la fracción VIII del artículo 116 de la Constitución Federal, en los siguientes términos:

> Las Constituciones de los Estados establecerán organismos autónomos, especializados, imparciales y colegiados, responsables de garantizar el

> derecho de acceso a la información y de protección de datos personales en posesión de los sujetos obligados, conforme a los principios y bases establecidos por el artículo 6º de esta Constitución y la ley general que emita el Congreso de la Unión para establecer las bases, principios generales y procedimientos del ejercicio de este derecho.

La LGTAIP, publicada en el *Diario Oficial de la Federación* (DOF) el 4 de mayo de 2015, ratifica el concepto jurídico de organismos garantes, considerándolos con autonomía constitucional especializados en materia de acceso a la información y protección de datos personales (artículo 3 fracción XVI).

Además, en el artículo 37 de dicha ley general, se precisa que los organismos garantes son sujetos autónomos, especializados, independientes, imparciales y colegiados, con personalidad jurídica y patrimonio propios, con plena autonomía técnica y de gestión, con capacidad para decidir sobre el ejercicio de su presupuesto, determinar su organización interna y responsables de garantizar (en el ámbito de su competencia) el ejercicio de los derechos de acceso a la información y la protección de datos personales conforme a los principios y bases establecidos por el artículo 6º de la Constitución federal, así como por lo previsto en dicha ley y demás disposiciones aplicables.

De un análisis e interpretación armónica de los principios y bases que marca la Constitución Federal en sus artículos 6º y 116, así como la LGTAIP, la LFTAIP, publicada en el DOF el 9 de mayo de 2016, y la LGPDPPSO que se comenta, en cuanto a la estructura y funciones de los organismos garantes, así como la integración, duración del cargo, requisitos, procedimiento de selección, régimen de incompatibilidades, excusas, renuncias, licencias y suplencias de los integrantes de dichos organismos, tenemos que, en uso de sus facultades legislativas, será obligación del Congreso de la Unión, los congresos de las entidades federativas y la Asamblea Legislativa de la Ciudad de México, garantizar la integración colegiada y autónoma de los organismos garantes, por lo que deberán prever en su conformación un número impar y sus integrantes se denominarán comisionados.

También se procurará que en la conformación de los comisionados se privilegie la experiencia en materia de acceso a la información pública y protección de datos personales e intentar mantener la equidad de género. La duración del cargo no será mayor a siete años y se realizará de manera escalonada para garantizar el principio de autonomía.

Durante el proceso de selección y para el nombramiento de los comisionados debe prevalecer, en todo momento, la transparencia, independencia y amplia participación de la sociedad. Además, en cuanto a su funcionamiento, los órganos garantes de las entidades federativas deben regirse por los principios

de certeza, legalidad, independencia, imparcialidad, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad.

En su artículo 2, la LGPDPPSO establece, entre sus objetivos, el de distribuir competencias entre los organismos garantes de la Federación y las entidades federativas en materia de protección de datos personales en posesión de sujetos obligados, función que se cumple en el artículo 91 de la citada norma.

## III. Análisis del contenido

Los organismos garantes tienen atribuciones o facultades que se pueden clasificar en dos dimensiones: judicial y administrativa.

En cuanto a la dimensión judicial, se identifican las siguientes:

a) Conocer, sustanciar y resolver, en el ámbito de sus respectivas competencias, los recursos de revisión interpuestos por los titulares en términos de lo dispuesto en la LGPDPPSO y demás disposiciones que resulten aplicables en la materia.

b) Presentar petición fundada al INAI para que conozca los recursos de revisión que por su interés y trascendencia así lo ameriten en términos de lo previsto en la LGPDPPSO y demás disposiciones que resulten aplicables en la materia.

c) Imponer las medidas de apremio para asegurar el cumplimiento de sus resoluciones.

d) Garantizar, en el ámbito de sus respectivas competencias, condiciones de accesibilidad para que los titulares que pertenecen a grupos vulnerables puedan ejercer, en igualdad de circunstancias, su derecho fundamental a la protección de datos personales.

e) Hacer del conocimiento de las autoridades competentes la probable responsabilidad derivada del incumplimiento de las obligaciones previstas en la ley y en las demás disposiciones que resulten aplicables.

f) Proporcionar al INAI los elementos que requiera para resolver los recursos de inconformidad que le sean presentados.

g) Según corresponda, interponer acciones de inconstitucionalidad en contra de leyes expedidas por las legislaturas de las entidades federativas que vulneren el derecho a la protección de datos personales.

Si bien la ley establece las atribuciones jurisdiccionales de los organismos garantes, es oportuno mencionar que en cuanto a la potestad sancionadora sólo se limita a imponer medidas de apremio para asegurar el cumplimiento de sus resoluciones y en caso de que se advierta una posible sanción, se debe solicitar al sujeto obligado el inicio de un procedimiento administrativo ajeno al ámbito de competencia de la LGPDPPSO.

El problema es hacer cumplir la sanción, pues es difícil determinar que las autoridades de la administración pública asuman la obligación de sancionar a los servidores públicos por violación a los derechos ARCO. Lo anterior se expresa desde la experiencia que se ha vivido en el país, donde los cargos públicos de los órganos garantes han sido determinados por los posibles sancionados. Además, los organismos garantes carecen de los medios coercitivos para hacer efectiva la sanción.

Las medidas de apremio que pueden imponer los organismos garantes consisten en una amonestación pública o multa equivalente a la cantidad de ciento cincuenta hasta mil quinientas veces el valor diario de la Unidad de Medida.

Así mismo, los organismos garantes deberán realizar los ajustes razonables para que los titulares que pertenecen a grupos vulnerables puedan ejercer, en igualdad de circunstancias, su derecho a la protección de datos personales realizando las modificaciones y adaptaciones necesarias y adecuadas que no impongan una carga desproporcionada o indebida.

A partir de la reforma publicada en el DOF el 29 de enero de 2016 al artículo 105, fracción II, de la Constitución le fue adicionado el *inciso h* en los siguientes términos:

> La Suprema Corte de Justicia de la Nación conocerá, en los términos que señale la ley reglamentaria, de los asuntos siguientes: […]
>
> II. De las acciones de inconstitucionalidad que tengan por objeto plantear la posible contradicción entre una norma de carácter general y esta Constitución.
>
> Las acciones de inconstitucionalidad podrán ejercitarse, dentro de los treinta días naturales siguientes a la fecha de publicación de la norma, por:
> […]
> h) El organismo garante que establece el artículo 6° de esta Constitución en contra de leyes de carácter federal y local, así como de tratados internacionales celebrados por el Ejecutivo Federal y aprobados por

el Senado de la República, que vulneren el derecho al acceso a la información pública y la protección de datos personales. Asimismo, los organismos garantes equivalentes en las entidades federativas, en contra de leyes expedidas por las Legislaturas locales.

Por lo anterior, los organismos garantes están legitimados para promover las acciones de inconstitucionalidad en contra de leyes expedidas por las legislaturas de las entidades federativas, que vulneren el derecho a la protección de datos personales.

En cuanto al ámbito de control administrativo, las facultades de los organismos garantes son:

a) Promover y difundir el ejercicio del derecho a la protección de datos personales.

b) Coordinarse con las autoridades competentes para que las solicitudes para el ejercicio de los derechos ARCO y los recursos de revisión que se presenten en lenguas indígenas sean atendidos en la misma lengua.

c) Elaborar y publicar estudios e investigaciones para difundir y ampliar el conocimiento sobre la materia de la LGPDPPSO.

d) Suscribir convenios de colaboración con el INAI para el cumplimiento de los objetivos previstos en la ley y demás disposiciones aplicables.

e) Vigilar, en el ámbito de sus respectivas competencias, el cumplimiento de la ley y demás disposiciones que resulten aplicables en la materia.

f) Llevar a cabo acciones y actividades que promuevan el conocimiento del derecho a la protección de datos personales, así como de sus prerrogativas.

g) Aplicar indicadores y criterios para evaluar el desempeño de los responsables respecto del cumplimiento de la ley y demás disposiciones que resulten aplicables.

h) Promover la capacitación y actualización en materia de protección de datos personales entre los responsables.

i) Solicitar la cooperación del Instituto en los términos de la ley.

j) Administrar, en el ámbito de sus competencias, la Plataforma Nacional de Transparencia.

k) Emitir, en su caso, las recomendaciones no vinculantes correspondientes a la Evaluación de impacto en protección de datos personales que le sean presentadas.

Para promover el ejercicio del derecho a la protección de datos personales es importante utilizar las herramientas que proporcionan las tecnologías de información y comunicación tales como cursos virtuales, aplicaciones informáticas en dispositivos tales como teléfonos celulares, computadoras personales, entre otros; así también se puede promover de forma institucional a través de convenios con el propósito de impartir cursos de capacitación dirigidos a diversos grupos sociales, valorando además las edades a las que están dirigidas.

Tratándose de solicitudes que sean presentadas en lengua indígena, los organismos garantes deben estar en comunicación permanente con las unidades de transparencia de los sujetos obligados, a efectos de que se respondan dichas solicitudes y se tramiten los recursos en la misma lengua en que fueron presentadas.

Una forma de coadyuvar a la transferencia de conocimiento en materia de datos personales es a través del apoyo en la publicación de estudios e investigaciones de impacto que permitan divulgar el tema de protección de datos para todos los sectores de la sociedad, por ejemplo, un manual para educación básica, un libro para educación superior, premios para mejores tesis de nivel posgrado y principalmente considerar las investigaciones de los académicos en esta esfera.

Una actividad permanente de los organismos garantes es vigilar el cumplimiento de la normatividad en materia de datos personales, tanto para los sujetos obligados que poseen la información, como para los titulares de dichos datos que quieran acceder al ejercicio de este derecho.

Una forma importante de vigilancia es el desarrollo de un instrumento de medición que permita evaluar los indicadores de desempeño de los sujetos obligados, entiéndase, responsables, tal como lo indica la ley, los cuales podrían diseñarse desde la unidad de transparencia o de los comités de transparencia con las funciones que tienen atribuidas, y su propósito es contar con un diagnóstico acerca del cumplimiento de la ley por parte de los sujetos obligados. Estos criterios pueden medirse a partir del desempeño de los responsables en el tratamiento de datos personales, mediante la observancia de los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, lo anterior puede permitir la certificación de calidad de los sujetos responsables cada determinado tiempo.

La administración de la Plataforma Nacional de Transparencia implica que los órganos garantes vigilen la actividad de los sujetos obligados de su entidad federativa correspondiente, a efectos de que realicen la actualización de su información en relación con la posibilidad de atender las solicitudes requeridas a través del nuevo sistema establecido.

La elaboración de una evaluación de impacto permite identificar riesgos para la privacidad, prevenir problemas y ofrecer alternativas de solución.[217] La evaluación de impacto en la protección de datos personales se identifica con un documento mediante el cual los sujetos obligados valoran los impactos reales respecto de determinado tratamiento de datos personales a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares. Los órganos garantes actúan como supervisores en cuanto a este tipo de documentos, dado que tienen la facultad de emitir resoluciones que son vinculatorias, definitivas e inatacables para los sujetos obligados.

Sin embargo, es importante que los sujetos obligados cuenten con la posibilidad de acudir ante los órganos garantes a solicitar una evaluación de impacto para que puedan adoptarse medidas de prevención adecuadas en relación con el tratamiento de datos que pueden suponer un riesgo para el titular.

## IV. Conclusiones

En el ámbito de la protección de datos personales adquiere imprescindible importancia la labor de los órganos autónomos especializados para la protección de este derecho a través de los órganos garantes, ello pone en evidencia el contraste de protección existente actualmente entre los países que dictaron normas sobre protección de datos de carácter personal y establecieron los órganos de control entre aquellos países que han dejado a cargo de los tribunales tradicionales y sin regulación específica esta actividad.

Cabe destacar que en el artículo segundo transitorio se previó que en caso de que el Congreso de la Unión o las legislaturas de las entidades federativas omitieran, total o parcialmente, realizar las adecuaciones legislativas que haya lugar en el plazo establecido de seis meses, resultaría aplicable, de manera directa, la LGPDPPSO, con la posibilidad de seguir aplicando de manera supletoria las leyes preexistentes en todo aquello que no se oponga a la misma. Hasta en tanto no se cumpla la condición impuesta en el citado artículo, esta precisión permite garantizar la protección de datos personales en todo el país, aun cuando no se cuente con la ley específica, en cada entidad o estado de la República Mexicana.

[217] Recio, M. (2016). "XXI. Aproximación basada en el riesgo, evaluación de impacto relativa a la protección de datos personales y consulta previa a la autoridad de control" en Piñar, J. (Dir.), Álvarez, M.y Recio, M. (Coords.), *Reglamento general de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Madrid: Ed. Reus.

Es muy cuestionable que los órganos garantes no puedan aplicar sanciones de forma directa a los responsables por la violación de la protección de los datos personales, delegando esta función, en definitiva, al interior de los propios sujetos obligados mediante sus órganos internos de control.

En el ámbito internacional se observa la importancia que se le otorga al control administrativo y jurisdiccional de los organismos garantes en materia de datos personales, lo anterior en virtud de la doctrina del margen de apreciación en el que cada estado puede emitir la normatividad que considere siempre y cuando tutele y proteja el contenido del derecho en cuestión.

## Referencias

Del Castillo, I. (2007). *Protección de datos: cuestiones constitucionales y administrativas (El derecho a saber y la obligación de callar)*. Navarra: Ed. Aranzadi-Thomson Civitas.

Grimalt, P. (2016). *La responsabilidad civil en el tratamiento automatizado de datos personales*. Granada: Ed. Comares.

Piñar, J. (Dir.), Álvarez, M. y Recio, M. (Coords.). (2016). *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Madrid: Ed. Reus.

Puccinelli, O. (2004). *Protección de datos de carácter personal*. Buenos Aires: Ed. Astrea.

Recio, M. (2016). "XXI. Aproximación basada en el riesgo, evaluación de impacto relativa a la protección de datos personales y consulta previa a la autoridad de control", en Piñar, J. (Dir.), Álvarez, M. y Recio, M. (Coords.) *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Madrid: Ed. Reus.

Verdaguer, J. y Bergas, M. (2010). *100 soluciones de protección de datos*. Valencia: Ed. Wolters Kluwer España.

DOF. (2014). Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, *Diario Oficial de la Federación*.

DOF. (2015). Ley General de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*.

DOF. (2016). Ley Federal de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*.

DOF. (2017). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, *Diario Oficial de la Federación*.

Parlamento Europeo y del Consejo. (2016). Reglamento (UE) 2016/679 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), *Diario Oficial de la Unión Europea*.

# CAPÍTULO III
# DE LA COORDINACIÓN Y PROMOCIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

***Artículo 92.*** *Los responsables deberán colaborar con el Instituto y los organismos garantes, según corresponda, para capacitar y actualizar de forma permanente a todos sus servidores públicos en materia de protección de datos personales, a través de la impartición de cursos, seminarios, talleres y cualquier otra forma de enseñanza y entrenamiento que se considere pertinente.*

***Artículo 93.*** *El Instituto y los Organismos garantes, en el ámbito de sus respectivas competencias, deberán:*

*I. Promover que en los programas y planes de estudio, libros y materiales que se utilicen en las instituciones educativas de todos los niveles y modalidades del Estado, se incluyan contenidos sobre el derecho a la protección de datos personales, así como una cultura sobre el ejercicio y respeto de éste;*

*II. Impulsar en conjunto con instituciones de educación superior, la integración de centros de investigación, difusión y docencia sobre el derecho a la protección de datos personales que promuevan el conocimiento sobre este tema y coadyuven con el Instituto y los Organismos garantes en sus tareas sustantivas, y*

*III. Fomentar la creación de espacios de participación social y ciudadana que estimulen el intercambio de ideas entre la sociedad, los órganos de representación ciudadana y los responsables.*

# COMENTARIO

**Gisela María Pérez Fuentes**

## I. Antecedentes

Con la primera LFTAIPG, publicada en el DOF el 11 de junio de 2002, misma que fue abrogada por la LFTAIP el 9 de mayo de 2016, podemos afirmar que desde el año 2002 se inició, de forma institucional, el proceso de formación de una cultura en materia de transparencia, acceso a la información pública y protección de datos personales. De la misma forma, los organismos garantes deben continuar sus trabajos de manera colaborativa con las instituciones educativas de todos los niveles, ello para impulsar y socializar el derecho fundamental a la protección de datos personales.

En otros países, en los que la protección de datos personales ha tenido un avance más significativo, se han desarrollado materiales mediante programas educativos, como recurso para la reflexión acerca de la importancia de la vida privada, el derecho a la intimidad y la protección de datos personales. De igual manera se ha dirigido el estudio de estos temas a docentes, padres de familia y estudiantes de educación primaria, secundaria, preparatoria y nivel superior.[218]

El programa antes mencionado, abarca conceptos de derechos y responsabilidades previstos en la legislación, persiguiendo, como objetivo, que el profesorado seleccione elementos de estos materiales, junto con otros recursos educativos, en distintas etapas del aprendizaje (educación básica, primaria y secundaria). De igual forma, los materiales podrán impartirse en diversas asignaturas tales como Educación ético-cívica, Educación para la ciudadanía y los derechos humanos, Tecnologías o Informática, entre otras. Un ejemplo de lo anterior lo podemos observar en países como España e Irlanda.

## II. Relevancia temática y contexto

Por lo que se refiere a la certificación en el derecho comparado, un modelo interesante es el que se ha establecido en España a través del esquema de certificación de delegados de Protección de datos. Así la Agencia Española de Protección de Datos (AEPD) en colaboración con la Entidad Nacional de Acreditación ha optado por promover un sistema de certificación, con el objetivo de ofrecer seguridad y fiabilidad, tanto a los profesionales de la privacidad como a las empresas y entidades que cuentan con esta figura al interior de su organización.[219]

---

[218] Agencia Española de Protección de Datos, Agencia de Protección de Datos de la Comunidad de Madrid y Agencia Catalana de Protección de Datos. (2007). *Proteger tu privacidad y controlar tus datos. Un recurso para el profesorado*. España: Hélice Creativos/Victoria Gasteiz.

[219] Cfr. Agencia Española de Protección de Datos. (2017). Disponible en: https://www.agpd.es/portalwebAGPD/temas/certificación/common/pdf/ESQUEMA_AEPD_DPD.pdf

La certificación propuesta en España se estructura en tres partes: la AEPD como propietaria y responsable del esquema, la Entidad Nacional de Acreditación como encargada de los requisitos que deben cumplir los certificadores y finalmente las propias entidades de certificación. Esta división a criterio de la Agencia Española es un factor de calidad para el proceso de certificación. La Agencia y la Entidad de Acreditación han suscrito un convenio de colaboración para coordinar sus actuaciones en el marco de sus respectivas actividades y competencias.

El modelo de certificación está acorde con el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, el cual establece una serie de medidas de responsabilidad activa por parte de aquellos que tratan datos para salvaguardar el derecho fundamental de los ciudadanos, siendo la certificación un mecanismo de garantía en dicho trabajo.

Por otra parte, hay que añadir la tendencia internacional al reconocimiento de la certificación en cualquier lugar del mundo siempre que haya sido realizada por los estándares de la Norma ISO/IEC 17024:2012. No obstante, como refieren Fernández y Recio, queda todavía un largo camino que debe considerar la acreditación de organizaciones de certificación, para que la protección de datos personales sea confiable.[220]

Ésta puede resultar una opción valorable en México para que el Instituto Nacional certifique a los responsables del tratamiento de datos personales que forman parte de la estructura administrativa de los sujetos obligados, dado que, además, es una de sus atribuciones establecidas en la LGPDPPSO. Esta certificación puede promoverse a través de los convenios de colaboración institucionales con entidades acreditadoras. La certificación no es la única vía, sin embargo, a partir de su implementación se otorgará más seguridad jurídica al trabajo desarrollado por los responsables del tratamiento y serviría como un elemento a considerar en el sistema de servicio profesional de carrera.

## III. Análisis del contenido

Para cumplir con los objetivos de la LGPDPPSO es imprescindible desarrollar la cultura de la protección de datos personales, para ello los responsables de las unidades de transparencia deben colaborar con los organismos garantes, para dar a conocer y preparar a todos los involucrados en el sistema y a la sociedad civil en la ponderación y utilidad democrática tanto del derecho de acceso a la información pública, como a la protección de datos personales que tienen en posesión los sujetos obligados, para ello es importante preparar un programa de

[220] Fernández, C. y Recio, M. (2016). "Certificado en protección de datos personales", en Piñar, J. (Dir.), Álvarez, M. y Recio, M. (Coords.), *Reglamento general de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Madrid: Ed. Reus.

capacitación continua que consista, precisamente, en la actualización sistemática y permanente de todos los servidores públicos en materia de protección de datos personales, por medio de cursos, seminarios, talleres y cualquier otra forma de enseñanza y entrenamiento que se considere pertinente.

Lo anterior es insuficiente si no se logra estabilidad funcional y especialización en la materia de tratamiento de datos pues hay que recordar que los organismos garantes cumplen una función administrativa y jurisdiccional, en tal sentido sería muy conveniente aplicar, en un primer momento, un proceso de certificación a los órganos garantes de los estados, y en una segunda fase, medir el desempeño de sus actividades y las estrategias para lograr la acreditación de los sujetos obligados en materia de protección de datos personales.

El INAI ha suscrito diversos convenios generales y específicos desde el año 2003 a la fecha, para efectos de la formación y capacitación continua a servidores públicos, así como a la sociedad civil. Entre ellos destacan, por ejemplo, el convenio con el Centro de Investigación y Docencia Económicas (CIDE), firmado en el año 2017, en el cual, el órgano garante de la Federación se comprometió, entre otras tareas, a:[221]

a) Organizar cursos, jornadas y talleres de capacitación dirigidas a la comunidad académica y estudiantil de los planteles de las universidades con el objetivo de promover un conocimiento útil y reproducible del derecho a la protección de datos personales. Estas dos palabras son imprescindibles a partir de la eficacia de los convenios.

b) Coadyuvar, en la medida de sus capacidades técnicas, a la inclusión de contenidos temáticos en programas de estudios impartidos por la institución educativa en cuestión.

c) Promover, de manera regular y permanente, la capacitación del personal académico y administrativo de la universidad sobre el tema de protección de datos personales.

d) Promover y desarrollar proyectos conjuntos de colaboración, a través de programas de apoyo a becarios o de programas de apoyo a estudiantes.

e) Garantizar que todos los beneficiarios sean elegidos sin ningún tipo de discriminación, ni de finalidad distinta a la de promover el derecho de protección de datos personales.

[221] Cfr. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2017). Disponible en: http://inicio.inai.org.mx/SitePages/ConveniosInstitucionales.aspx

f) Expedir constancias a quienes cursan alguno de los programas impartidos en caso de que así lo ameriten. Por ejemplo, se citan los convenios que el Instituto ha celebrado con la Universidad Autónoma del Estado de Morelos y con la Universidad del Estado de Guanajuato.[222]

Estos convenios suscritos con diversas instituciones de educación superior permiten, fundamentalmente, el desarrollo del conocimiento e investigación básica, que de acuerdo con el Consejo Nacional de Ciencia y Tecnología es aquella que genera conocimiento de frontera y contribuye a mejorar la calidad de la educación superior, así como la formación de científicos y académicos.[223]

El INAI ha suscrito otros convenios que potencian la investigación aplicada. Un ejemplo es el que se firmó con el Instituto Latinoamericano de la Comunicación Educativa (ILCE)[224] que considera en sus objetivos los siguientes:

a) Producción o coproducción de materiales audiovisuales e impresión de carácter didáctico.

b) Diseño y desarrollo de iniciativas y herramientas que facilitan el conocimiento y difusión de los derechos de acceso a la información y protección de datos a la población.

c) Desarrollo de plataformas tecnológicas para espacios virtuales de aprendizaje diseñadas para la actualización y toma de decisiones virtuales.

d) Fomento y apoyo al intercambio de experiencias, datos estadísticos y materiales informativos.

e) Promoción y diseño de una estrategia para realizar o apoyar producciones o coproducciones audiovisuales con el objetivo de difundir y desarrollar el conocimiento de los derechos de acceso a la información y protección de datos.

f) Conformar publicaciones periódicas de difusión y divulgación científica en materia de protección de datos, tratando que dichos materiales sean a la vez accesibles a la ciudadanía, pero con calidad técnica.

g) Asesoría científica y técnica recíproca para el cumplimiento de programas,

---

[222] *Idem.*

[223] Consejo Nacional de Ciencia y Tecnología. (2016). *Convocatoria de Investigación Científica Básica 2016*.[Archivo PDF]. Disponible en: https://www.conacyt.gob.mx/index.php/el-conacyt/convocatorias-y-resultados-conacyt/convocatorias-fondos-sectoriales-constituidos/convocatoria-sep-conacyt/investigacion-basica-sep/abierta-investigacion-basica/convocatoria-de-investigacion-cientifica-basica-2016/13376-convocatoria-investigacion-cientifica-basica-2016/file, [fecha de consulta: 6 de mayo 2018].

[224] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2017). Disponible en: http://inicio.inai.org.mx/SitePages/ConveniosInstitucionales.aspx

actividades, objetivos o funciones que desarrollen al interior de sus respectivas instituciones. Este tipo de convenio se identifica como específico de colaboración y proyectos estratégicos.

Este trabajo loable del órgano garante federal, de suscribir convenios de colaboración que impulsen conocimientos e investigaciones, tanto básicas como aplicadas, debe ser replicado por los organismos garantes de las entidades federativas. El Instituto debe trazar lineamientos de lo que realmente se debe perseguir, pues es conocido que en las entidades federativas el acuerdo político dificulta el desarrollo técnico y especializado que debe primar en la materia, tanto de transparencia y acceso a la información como de protección de datos personales y los obstáculos que encuentran los organismos garantes de los estados cuando realmente quieren desarrollar este trabajo.

Por eso se considera que, atendiendo a la experiencia del Instituto, se debe avanzar un paso más en este proceso sistemático y continuo de capacitación con el objeto de potenciar el servicio profesional existente, por ejemplo, a través del Estatuto del Servicio Profesional en el Instituto Federal de Acceso a la Información y Protección de Datos (ahora INAI) que fue publicado en el DOF el 2 de julio de 2013, haciendo extensivo este mecanismo para los estados, evitando así la improvisación y salto del personal de una actividad ajena a los objetivos que persiguen estos organismos garantes para llenar cuotas de poder político o relaciones de carácter personal.

La situación anterior podría ser tolerable si los funcionarios se encuentran certificados para desempeñar estas actividades, sin embargo, de nada sirve la capacitación cuando en algunas ocasiones ha ocurrido que los puestos son ocupados por personas ajenas al sistema de formación en el derecho de acceso a la información pública, la transparencia y los datos personales.

Destaco, en este sentido, el objetivo que se ha perseguido con el Estatuto del Servicio Profesional del Instituto en cuanto a:

a) Regular la planeación, organización, gestión y administración del servicio profesional en el Instituto, con respecto al ingreso y movilidad, aprendizaje y desarrollo, evaluación del desempeño, otorgamiento de estímulos y licencias, causas de separación y medios de defensa de sus miembros.

b) Los principios rectores que deben estar presentes en la formación de servidores públicos profesionales en materia de acceso a la información y protección de datos personales son: la honestidad, la ética, la transparencia, la objetividad, la legalidad, la imparcialidad, la calidad profesional, la equidad, la eficiencia y el mérito profesional.

c) Son sujetos y se rigen por el servicio profesional todos los puestos de director general, director de área, subdirector de área y jefe de Departamento adscritos a las direcciones generales.

Se exceptúan, en los puestos como servidores de carrera: el personal adscrito a las oficinas de los comisionados; el personal adscrito a las oficinas de los secretarios de Acceso a la Información, de Protección de Datos Personales y General del Instituto; el secretario técnico del Pleno y el personal adscrito a su oficina; el director general de Administración, el director de Desarrollo Humano y Organizacional, el subdirector del Servicio Profesional y el jefe de Departamento de Selección de Personal; y el director general de Comunicación Social y Difusión. Considero que para una mayor rendición de cuentas, algunos de estos puestos también deberían someterse al procedimiento de oposición para los servidores de carrera.

d) Considerar el concurso de oposición como el procedimiento de selección para ocupar puestos vacantes que formen parte del servicio profesional será este procedimiento el único a través del cual se selecciona al personal idóneo para ocupar puestos vacantes de la estructura.

e) La existencia de una Comisión Supervisora de la Gestión del Servicio Profesional en el Instituto.

La Comisión Supervisora tendrá entre sus atribuciones conocer y resolver, en su carácter de autoridad, los siguientes procedimientos:

a) De revisión interpuesto por los miembros del servicio profesional para inconformarse en contra de los resultados de los concursos de oposición, del aprendizaje y desarrollo, de la evaluación del desempeño, del otorgamiento de estímulos y la negativa al otorgamiento de licencias.

b) De revisión interpuesto por los candidatos para inconformarse en contra de los resultados de los concursos de oposición en los que participen.

c) El definido para que los nombramientos de los miembros del servicio profesional dejen de surtir efectos.

La Comisión Supervisora debe establecer (por medio de criterios objetivos) los lineamientos derivados del proceso de elección de los puestos del servicio profesional. La organización del servicio profesional no puede ser improvisada, por ello, en el caso del Instituto Nacional, se ha establecido que el órgano de gobierno definirá y expedirá los instrumentos jurídicos necesarios para la gestión y administración del servicio profesional, destacando de manera enunciativa un catálogo general de funciones y puestos así como distintos lineamientos que incluyan el ingreso y la movilidad, el desempeño y los

procedimientos de revisión de resultados, así como los necesarios para, en su caso, establecer alguna separación de los miembros del servicio profesional, lo anterior conforme lo establece el artículo 13 del Estatuto del Servicio Profesional en el Instituto.

En este comentario se propone hacer extensivo el servicio profesional como el conjunto de principios, normas, programas y procedimientos que se utilizan para garantizar la igualdad de oportunidades en el acceso a la función pública, con base en el mérito y el desempeño y con el fin de impulsar el desarrollo profesional de los servidores públicos en beneficio de la sociedad a los organismos garantes de la República Mexicana.

Por último, debe fomentarse la creación de espacios de participación social y ciudadana que estimulen el intercambio de ideas entre la sociedad, los órganos de representación ciudadana y los responsables.

Lo anterior puede estimularse a través de diversas opciones tales como: cursos presenciales y virtuales, ferias, programas de radio y televisión, así también estimular la participación ciudadana en concursos sobre la protección de datos personales, estableciendo distintas categorías que contemplen a niños, jóvenes universitarios y a la sociedad civil en general.

Un ejemplo de estos premios son los desarrollados por los organismos garantes de protección de datos, la AEPD en el caso de España, la cual otorga todos los años el premio a las buenas prácticas educativas en privacidad y protección de datos personales para un uso seguro de internet, cuyo propósito consiste en premiar la adopción de buenas prácticas que promuevan el conocimiento del derecho fundamental a la protección de datos, así como contribuir a crear consciencia sobre el valor de la privacidad y el uso responsable de la información que se comparte en internet. El resultado de estos premios permitirá generar la participación ciudadana a través de espacios de intercambio en los ámbitos nacional y estatal.

Otra manera de fomentar la creación de espacios de participación social y ciudadana que estimulen el intercambio de ideas entre la sociedad, los órganos de representación ciudadana y los responsables, puede darse mediante el desarrollo de códigos de conducta o de buenas prácticas, en los cuales se reflejan los principios básicos en materia de protección de datos personales para asegurar y mejorar el cumplimiento y aplicación de este derecho.

Lo anterior coincide con lo que sostiene Díaz-Romeral cuando afirma que los códigos de conducta deben aportar un valor añadido en términos de claridad, abordar adecuadamente la problemática específica del tratamiento en un sector específico y aportar soluciones. En decir, deben generar confianza. Por ejemplo,

en el derecho comparado español se encuentra el código tipo de protección de datos para organizaciones sanitarias privadas, como un instrumento que aporta valor añadido a la normatividad vigente (Díaz-Romeral, 2016).

Con independencia de que es una atribución del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, prevista en el artículo 14, fracción XV, de la LGPDPPSO estos códigos pueden desarrollarse a través de un grupo de trabajo en el que participen representantes de los organismos garantes, representantes de los responsables y sociedad civil organizada especializada en estos temas, lo que coadyuva a la construcción de una sociedad democrática donde se respeten todos los derechos humanos y por supuesto, la privacidad es uno de aquellos que permite la realización de la persona.

## IV. Conclusiones

En materia de datos personales están abiertas una serie de posibilidades en las que deben considerarse proyectos de investigación en su vertiente básica y aplicada con financiamientos mixtos en materia de protección de datos personales, tanto con instituciones nacionales como extranjeras con experiencia en la forma de divulgar el conocimiento de este derecho.

Son loables las iniciativas en la materia que se ha tenido con instituciones de educación superior y con reconocido prestigio, estableciendo una serie de convenios que permiten desarrollar conocimiento científico básico y aplicado pero es preciso señalar que un área de oportunidad para el Instituto y los organismos garantes es la integración de centros de investigación en conjunto con las instituciones de educación superior que incluyen, en sus planes y programas de estudios a nivel posgrado, asignaturas sobre protección de datos personales y derecho a la privacidad.

Esta área de oportunidad se hace más eficaz cuando esos posgrados se encuentran certificados por el Consejo Nacional de Ciencia y Tecnología, es decir, pertenecen al Programa Nacional de Posgrados de Calidad, pero que, además, potencian el desarrollo de investigaciones en temas de frontera como es la protección de datos personales.

Otra estrategia imprescindible para la concienciación y cultura en materia de protección de datos personales es la elaboración de códigos de conducta o buenas prácticas que otorguen confianza y efectos favorables a las partes que intervienen en el tratamiento de datos personales, tanto para los sujetos obligados como para el titular de la información.

La capacitación y el desarrollo de investigaciones en temas de frontera sobre protección de datos personales debe ser una actividad continua y permanente que se promueva por los órganos garantes, tanto en el ámbito federal como de los órganos garantes de los estados, en vinculación con entidades educativas y certificadoras, así también se debe contar con la participación de la sociedad civil organizada.

## Referencias

Agencia Española de Protección de Datos, Agencia de Protección de Datos de la Comunidad de Madrid y Agencia Catalana de Protección de Datos. (2007). *Proteger tu privacidad y controlar tus datos. Un recurso para el profesorado*. España: Hélice Creativos/Victoria Gasteiz.

Agencia Española de Protección de Datos. (2017). Disponible en: https://www.agpd.es/portalwebAGPD/temas/certificación/common/pdf/ESQUEMA_AEPD_DPD.pdf.

Consejo Nacional de Ciencia y Tecnología. (2016). *Convocatoria de Investigación Científica Básica 2016*.[Archivo PDF]. Disponible en: https://www.conacyt.gob.mx/index.php/el-conacyt/convocatorias-y-resultados-conacyt/convocatorias-fondos-sectoriales-constituidos/convocatoria-sep-conacyt/investigacion-basica-sep/abierta-investigacion-basica/convocatoria-de-investigacion-cientifica-basica-2016/13376-convocatoria-investigacion-cientifica-basica-2016/file, [fecha de consulta: 6 de mayo 2018].

Del Castillo, I. (2007). *Protección de datos: cuestiones constitucionales y administrativas (El derecho a saber y la obligación de callar)*. Navarra: Ed. Aranzadi/Thomson Civitas.

DOF. (2014). Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, *Diario Oficial de la Federación*.

DOF. (2015). Ley General de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*.

DOF. (2016) Ley Federal de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*.

DOF. (2017). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, *Diario Oficial de la Federación*.

Grimalt, P. (2016). *La responsabilidad civil en el tratamiento automatizado de datos personales*. Granada: Ed. Comares.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2017). Convenios Institucionales. Disponible en: http://inicio.inai.org.mx/SitePages/ConveniosInstitucionales.aspx, [fecha de consulta: 6 de mayo 2018).

Piñar, J. (Dir.), Álvarez, M. y Recio, M. (Coords.). (2016). *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Madrid: Ed. Reus.

Puccinelli, O. (2004). *Protección de datos de carácter personal*. Buenos Aires: Ed. Astrea.

Recio, M. (2016). "XXI. Aproximación basada en el riesgo, evaluación de impacto relativa a la protección de datos personales y consulta previa a la autoridad de control" en Piñar, J. (Dir.), Álvarez, M. y Recio, M. (Coords.), *Reglamento general de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*. Madrid: Ed. Reus.

Recio, M. (2016). *Protección de datos personales e innovación: ¿(in) compatibles?*. Madrid: Ed. Reus.

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), *Diario Oficial de la Unión Europea,* L 119, el 4 de mayo de 2016.

Verdaguer, J. y Bergas, M. (2010). *100 soluciones de protección de datos*. Valencia: Ed. Wolters Kluwer España.

# TÍTULO NOVENO

# DE LOS PROCEDIMIENTOS DE IMPUGNACIÓN EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS

# CAPÍTULO I
# DISPOSICIONES COMUNES A LOS RECURSOS DE REVISIÓN Y RECURSOS DE INCONFORMIDAD

***Artículo 94.*** *El titular o su representante podrá interponer un recurso de revisión o un recurso de inconformidad ante el Instituto o los Organismos garantes, según corresponda, o bien, ante la Unidad de Transparencia, a través de los siguientes medios:*

*I. Por escrito libre en el domicilio del Instituto o los Organismos garantes, según corresponda, o en las oficinas habilitadas que al efecto establezcan;*

*II. Por correo certificado con acuse de recibo;*

*III. Por formatos que al efecto emita el Instituto o los Organismos garantes, según corresponda;*

*IV. Por los medios electrónicos que para tal fin se autoricen, o*

*V. Cualquier otro medio que al efecto establezca el Instituto o los Organismos garantes, según corresponda.*

*Se presumirá que el titular acepta que las notificaciones le sean efectuadas por el mismo conducto que presentó su escrito, salvo que acredite haber señalado uno distinto para recibir notificaciones.*

***Artículo 95.*** *El titular podrá acreditar su identidad a través de cualquiera de los siguientes medios:*

*I. Identificación oficial;*

*II. Firma electrónica avanzada o del instrumento electrónico que lo sustituya, o*

*III. Mecanismos de autenticación autorizados por el Instituto y los Organismos garantes, según corresponda, publicados mediante*

*acuerdo general en el Diario Oficial de la Federación o en los diarios y gacetas oficiales de las Entidades Federativas.*

*La utilización de la firma electrónica avanzada o del instrumento electrónico que lo sustituya eximirá de la presentación de la copia del documento de identificación.*

***Artículo 96.*** *Cuando el titular actúe mediante un representante, éste deberá acreditar su personalidad en los siguientes términos:*

*I. Si se trata de una persona física, a través de carta poder simple suscrita ante dos testigos anexando copia de las identificaciones de los suscriptores, o instrumento público, o declaración en comparecencia personal del titular y del representante ante el Instituto.*

*II. Si se trata de una persona moral, mediante instrumento público.*

***Artículo 97.*** *La interposición de un recurso de revisión o de inconformidad de datos personales concernientes a personas fallecidas, podrá realizarla la persona que acredite tener un interés jurídico o legítimo.*

***Artículo 98.*** *En la sustanciación de los recursos de revisión y recursos de inconformidad, las notificaciones que emitan el Instituto y los Organismos garantes, según corresponda, surtirán efectos el mismo día en que se practiquen.*

*Las notificaciones podrán efectuarse:*

*I. Personalmente en los siguientes casos:*

*a) Se trate de la primera notificación;*

*b) Se trate del requerimiento de un acto a la parte que deba cumplirlo;*

*c) Se trate de la solicitud de informes o documentos;*

*d) Se trate de la resolución que ponga fin al procedimiento de que se trate, y*

*e) En los demás casos que disponga la ley;*

*II. Por correo certificado con acuse de recibo o medios digitales o sistemas autorizados por el Instituto o los Organismos garantes, según corresponda, y publicados mediante acuerdo general en el Diario Oficial de la Federación o diarios o gacetas oficiales de las Entidades Federativas, cuando se trate de requerimientos, emplazamientos, solicitudes de informes o documentos y resoluciones que puedan ser impugnadas;*

*III. Por correo postal ordinario o por correo electrónico ordinario cuando se trate de actos distintos de los señalados en las fracciones anteriores, o*

*IV. Por estrados, cuando la persona a quien deba notificarse no sea localizable en su domicilio, se ignore éste o el de su representante.*

***Artículo 99.*** *El cómputo de los plazos señalados en el presente Título comenzará a correr a partir del día siguiente a aquél en que haya surtido efectos la notificación correspondiente.*

*Concluidos los plazos fijados a las partes, se tendrá por perdido el derecho que dentro de ellos debió ejercitarse, sin necesidad de acuse de rebeldía por parte del Instituto.*

**Artículo 100.** *El titular, el responsable y los Organismos garantes o cualquier autoridad deberán atender los requerimientos de información en los plazos y términos que el Instituto y los Organismos garantes, según corresponda, establezcan.*

***Artículo 101.*** *Cuando el titular, el responsable, los Organismos garantes o cualquier autoridad se nieguen a atender o cumplimentar los requerimientos, solicitudes de información y documentación, emplazamientos, citaciones o diligencias notificadas por el Instituto o los Organismos garantes, según corresponda, o facilitar la práctica de las diligencias que hayan sido ordenadas, o entorpezca las actuaciones del Instituto o los Organismos garantes, según corresponda, tendrán por perdido su derecho para hacerlo valer en algún otro momento del procedimiento y el Instituto y los Organismos garantes, según corresponda, tendrán por ciertos los hechos materia del procedimiento y resolverá con los elementos que disponga.*

***Artículo 102.*** *En la sustanciación de los recursos de revisión o recursos de inconformidad, las partes podrán ofrecer las siguientes pruebas:*

*I. La documental pública;*

*II. La documental privada;*

*III. La inspección;*

*IV. La pericial;*

*V. La testimonial;*

*VI. La confesional, excepto tratándose de autoridades;*

*VII. Las imágenes fotográficas, páginas electrónicas, escritos y demás elementos aportados por la ciencia y tecnología, y*

*VIII. La presuncional legal y humana.*

*El Instituto y los Organismos garantes, según corresponda, podrán allegarse de los medios de prueba que consideren necesarios, sin más limitación que las establecidas en la ley.*

## COMENTARIO

**Ana Elena Fierro**

### I. Antecedentes

La protección de los datos personales, sea en manos de los particulares o de los sujetos obligados, es un derecho humano consagrado en la Constitución. El derecho a la protección de datos personales tiene como fin garantizar la privacidad de las personas y la prerrogativa a su autodeterminación informativa.[225] El artículo 6º de la CPEUM establece los principios, directrices y reglas básicas sobre las cuales se construyen los sistemas de protección de datos personales. Asimismo, mandata la creación de órganos garantes encargados de la promoción y protección de los derechos de acceso a la información pública y protección de datos personales. También la Constitución ordena una especial protección de información respecto a la identidad y datos personales de las víctimas y ofendidos partes en el procedimiento penal (artículo 20, apartado C, fracción V constitucional).[226]

El artículo 6º constitucional, apartado A, fracción II señala que la información que se refiere a la vida privada de las personas y los datos personales será protegida en los términos y con las excepciones que fijen las leyes. Como parte del cumplimiento de este mandato constitucional se emitió la LGPDPPSO.

Ahora bien, para que el ejercicio de un derecho humano sea efectivo resulta indispensable que las personas cuenten con mecanismos para

[225] DERECHO HUMANO A LA PROTECCIÓN DE DATOS PERSONALES. SE VULNERA EN PERJUICIO DE LOS MENORES DE EDAD CON MOTIVO DE LA PUBLICACIÓN DE SUS DATOS PERSONALES Y SENSIBLES EN EL PORTAL DE INTERNET DE LA PROCURADURÍA GENERAL DE JUSTICIA DEL ESTADO DE QUERÉTARO, A TRAVÉS DE SU DEPARTAMENTO DE LOCATEL, A PROPÓSITO DE LA PETICIÓN DE UN PARTICULAR, QUE NO SE UBIQUE EN ALGUNA DE LAS HIPÓTESIS PARA CONSIDERAR QUE SE ENCUENTRAN EN RIESGO INMINENTE DE SUFRIR DAÑO GRAVE EN SU INTEGRIDAD PERSONAL. Suprema Corte de Justicia de la Nación. Tesis XXII.1o.1 CS, Décima Época, *Semanario Judicial de la Federación y su Gaceta*, febrero de 2016, Tomo III, p. 2060.

[226] SISTEMAS DE PROTECCIÓN DE DATOS PERSONALES Y DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA. PRECEPTOS CONSTITUCIONALES QUE LOS REGULAN. Tribunales Colegiados de Circuito. Tesis I.2o.A.E.1 CS, Décima Época, *Semanario Judicial de la Federación y su Gaceta*, Libro 39, febrero de 2017, p. 2364.

exigir su cumplimiento, de lo contrario, ante la negativa de una autoridad de proteger un derecho o de un sujeto obligado a garantizar la protección de los datos personales, el particular quedaría indefenso. Al efecto, la LGPDPPSO establece en su Título Noveno un conjunto de recursos a cargo de los órganos garantes en particular del INAI para que las personas acudan a demandar la protección de sus datos personales o el ejercicio de los derechos ARCO.

Los siguientes párrafos analizan los procedimientos de impugnación establecidos en los artículos 94 al 102 de la LGPDPPSO, en materia de protección de datos personales en posesión de sujetos obligados, en particular las disposiciones comunes a los recursos de revisión e inconformidad. Para ello se lleva a cabo un análisis del concepto jurídico del recurso, sus alcances y limitaciones para, posteriormente, compararlo con los recursos establecidos por la LGPDPPSO y la jurisprudencia aplicable, enfatizando sus fortalezas y áreas de oportunidad.

## II. Relevancia temática y contexto

El principio de legalidad que rige a toda actuación de los órganos de Estado implica que el particular tiene derecho a que cualquier autoridad al momento de actuar cumpla con los siguientes requisitos: que tenga competencia para hacerlo y que se apegue a las formalidades, motivo, objeto y fin prescritos por la ley. Para proteger este cúmulo de derechos derivados del principio de legalidad existen medios, otorgados a su titular, cuya finalidad es lograr el retiro, la reforma o la anulación del acto contrario al derecho.[227] Estos procedimientos se dan por la vía administrativa a través de recursos como los de revisión e inconformidad, o bien, por la vía jurisdiccional mediante procesos de control de legalidad o constitucionalidad. El maestro Fraga define el recurso administrativo como un medio legal del que dispone un particular afectado en sus derechos o intereses por un acto administrativo. Éste, a su vez, se subdivide en revocación o reconsideración —también llamada revisión ante la autoridad superior, oposición o inconformidad.[228]

Tradicionalmente la doctrina ha clasificado a estos recursos en dos clases: los indirectos, que son medios de “autotutela” que la administración desarrolla en su propio seno y están destinados a garantizar la eficiencia de la administración y sólo por efecto reflejo representan una garantía para el particular, en estos medios la autoridad está legalmente obligada a intervenir y examinar nuevamente, en cuanto a su legalidad u oportunidad, la actuación objeto de la queja. Respecto de estos recursos administrativos suelen distinguirse aquellos que se interponen ante una autoridad jerárquica superior o los que son resueltos por un órgano administrativo determinado al efecto.

[227] Fraga, G. (2000). *Derecho administrativo*. México: Porrúa.
[228] *Ibíd.*, p. 441.

Por su parte, los recursos directos son medios que sí están destinados en forma inmediata a satisfacer el interés privado.[229] Además, dependiendo de las autoridades que intervienen, se clasifican en recursos administrativos y acciones jurisdiccionales. A su vez, es importante distinguir los recursos que conoce y resuelve una instancia administrativa diferente a la que emitió el acto impugnado, es decir, los recursos y acciones ante tribunales administrativos o las acciones propiamente dichas ante los tribunales comunes. Estos recursos directos suelen denominarse *recurso de revisión* o el *recurso de inconformidad*, términos que varían dependiendo de la ley de que se trate.[230]

En ese sentido, parecen existir en la doctrina divergencias respecto de la finalidad de los recursos administrativos. Sánchez Pichardo distingue que la finalidad procesal de una autoridad judicial está en juzgar a dos partes contradictorias (que es lo que compone a un conflicto), mientras que la finalidad administrativa es la de desarrollar un interés en conflicto para contrastarlo en el *autoexamen* contra el parámetro legal que enmarca su actuación. Sólo en este contraste se decide confirmar o revocar el acto administrativo. Por ello, el recurso administrativo no es una instancia contenciosa en estricto sentido,[231] más bien, lo que se busca es dar a las personas la posibilidad de obtener una decisión a través de un proceso y ante una instancia neutral e independiente.[232] De donde se concluye que el recurso administrativo, más que una garantía para el administrado es un beneficio de la administración[233] cuya finalidad es "que los errores y excesos de la administración pública, en perjuicio de los particulares, sean corregidos por ella misma, sin la intervención de otros órganos del poder público, lo que permite explicarlo como autocontrol". [234]

Una segunda postura es aquella que reconoce que cuando es una autoridad independiente la que resuelve la validez del acto administrativo, los recursos también pueden ser entendidos como un medio de defensa del administrado, que tienen como finalidad fundamental corregir los actos de la autoridad administrativa que el particular considera contrarios a su derecho.[235] A su vez, el objeto del recurso administrativo es controlar la actividad de la autoridad para que ésta se ajuste al principio de legalidad. Sin embargo, dicho objeto no es sólo el control que puede ejercer el particular, sino que también implica una limitación de las atribuciones discrecionales del emisor del acto administrativo.[236] Es decir, es una forma de control jurisdiccional sobre la autoridad administrativa, una

[229] Sánchez, A. (2006). *Los medios de impugnación en materia administrativa*. México: Porrúa.
[230] *Ibíd.*, p. 121.
[231] *Idem.*
[232] García de Enterría, E. y Fernández, T. (2011). *Curso de derecho administrativo*, Tomo II, España: Thompson Reuters, p. 537.
[233] *Idem.*
[234] Fernández, J. (2005). *Derecho administrativo y administración pública*. México: UNAM, Porrúa.
[235] Armienta, G. (2012). *Tratado Teórico Práctico de los Recursos Administrativos*. México: Porrúa, p. 57.
[236] *Idem.*

expresión de tendencia hacia la protección de los derechos e intereses de los administrados, y es una forma de centralización del control administrativo.[237] En suma, los recursos administrativos directos constituyen herramientas en manos de los particulares, mediante los cuales, pueden exigir que las autoridades rindan cuentas de su actuación, al establecerse como mecanismos de control del cumplimiento del principio de legalidad.[238]

## III. Análisis del contenido

Los recursos establecidos en la LGPDPPSO tienen la particularidad de que su objeto es la protección de un derecho humano encomendado a órganos constitucionales autónomos creados con esta finalidad. De modo que, si bien es cierto que sirven como medios correctivos de la actuación de los sujetos obligados, también son procedimientos que garantizan la eficacia del derecho de protección de datos personales y la autodeterminación informativa de las personas. Estos nuevos recursos, en manos de órganos constitucionales autónomos, no han sido tradicionalmente abordados por la doctrina del derecho administrativo, por lo que hoy en día podríamos considerar a este tipo de recursos en una tercera clasificación como procedimientos directos cuasi jurisdiccionales.

La Suprema Corte de Justicia de la Nación (SCJN) ha señalado que, dada la especial naturaleza de la materia regulada por las leyes derivadas del artículo 6° constitucional, la importancia de dar celeridad y evitar procedimientos gravosos en el ejercicio de estos derechos, dichos actos administrativos no deben ser revisados por los tribunales contenciosos, sino por órganos especializados constitucionalmente y diseñados para ese efecto.[239] De ahí que se propone considerarlos como en un tercer grupo al ser de carácter cuasi jurisdiccional y tener por objeto principal la garantía de los derechos humanos consagrados en el artículo 6° constitucional. Así los ha caracterizado también la SCJN al señalar que, si bien los recursos no son actos plenos de impartición de justicia, sí tienen una función de control de la actuación de las autoridades para la protección de los particulares, por lo tanto, deben responder a los principios de acceso a la justicia y justicia pronta y expedita mandatados por el artículo 17 constitucional.[240] Tales preceptos resultan aplicables, también, a los recursos en

[237] *Ibíd.*, p. 54.

[238] Fierro, A. (2017). *El Sistema Normativo de Rendición de Cuentas y el Ciclo del Uso de los Recursos Públicos en el Orden Jurídico Mexicano* (Tesis doctoral). México: Instituto de Investigaciones Jurídicas de la UNAM.

[239] TRIBUNAL FEDERAL DE JUSTICIA FISCAL Y ADMINISTRATIVA. ES INCOMPETENTE PARA CONOCER DE LAS RESOLUCIONES RECAÍDAS AL RECURSO DE REVISIÓN PREVISTO EN LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL. Tribunales Colegiados de Circuito I.13o.A.142 A, Novena Época, *Semanario Judicial de la Federación y su Gaceta*, Tomo XXVI, octubre de 2007, p. 3349.

[240] MEDIOS DE IMPUGNACIÓN DE UN ACTO ADMINISTRATIVO. CUANDO LA AUTORIDAD EMISORA INFORMA AL PARTICULAR LA PROCEDENCIA INDISTINTA DE UNO ORDINARIO Y OTRO EXTRAORDINARIO, SE ACTUALIZA UNA EXCEPCIÓN AL PRINCIPIO DE DEFINITIVIDAD

manos de los órganos garantes, que si bien, no se constituyen como tribunales, propiamente dichos, sí tienen entre sus competencias la de garantizar que los sujetos obligados cumplan con las responsabilidades derivadas de los derechos de protección de datos y acceso a la información pública.[241] En esta misma línea, el dictamen del Senado de la LGPDPPSO señala que ésta tiene como propósito proveer a las personas "de herramientas jurídicas que les permitan imponer un límite a las actuaciones de las autoridades que pudieran conculcar la esfera de sus derechos" relacionados con el tratamiento de sus datos personales.[242]

Continuando con el maestro Gabino Fraga, podemos justificar que los recursos establecidos en la LGPDPPSO se tratan de actos cuasi jurisdiccionales, en virtud de que, si bien son competencia de órganos constitucionalmente autónomos y no de tribunales, cumplen con las siguientes características:

1. El fin de la controversia parte de la decisión de la administración, en este caso de un sujeto obligado, a efecto de determinar si constituye una violación a la ley. En el caso que nos ocupa a la LGPDPPSO.
2. Que las normas que determinan el recurso establecen las garantías mínimas del debido proceso. En este caso, tanto el recurso de revisión como el de inconformidad presentan las etapas de demanda, contestación, presentación de pruebas, alegatos y resolución.
3. Que el particular puede recurrir la resolución del recurso en la vía constitucional. En este caso el artículo 116 de la LGPDPPSO señala que el particular puede acudir al juicio de amparo.[243]

Este criterio también se apoya en los precedentes de la SCJN que estiman que los recursos ante órganos especializados son actos materialmente jurisdiccionales[244] que deben seguir los principios del artículo 17 constitucional,[245] hecha la salvedad de que también deben adecuarse a la

PARA LA PROCEDENCIA DEL JUICIO DE AMPARO. Tribunales Colegiados de Circuito. Tesis XVI.1o.A.135 A, *Semanario Judicial de la Federación y su Gaceta*, Libro 45, agosto de 2017, Tomo IV, p. 2928.

[241] RECURSO DE REVISIÓN PREVISTO EN LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL. PARA SU PROCEDENCIA NO DEBE EXIGIRSE AL PARTICULAR EL USO DE EXPRESIONES SACRAMENTALES O DE FORMALIDADES INNECESARIAS O EXAGERADAS. Tribunales Colegiados de Circuito. Tesis .2o.A.E.20 A, *Semanario Judicial de la Federación y su Gaceta*, Libro 20, Tomo II, julio de 2015, p. 755.

[242] Cámara de Diputados. (2015) p. 57. [Archivo PDF]. Disponible en: http://www.senado.gob.mx/comisiones/gobernacion/docs/proteccion_datos/Documento3.pdf, [fecha de consulta: 7 de mayo 2018].

[243] Fraga, G. (2000). *Derecho administrativo*. México: Porrúa.

[244] ADMINISTRACIÓN DE JUSTICIA. EL ARTÍCULO 17 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS ESTABLECE DIVERSOS PRINCIPIOS QUE INTEGRAN AQUEL DERECHO PÚBLICO SUBJETIVO, A CUYA OBSERVANCIA ESTÁN OBLIGADAS LAS AUTORIDADES QUE REALIZAN ACTOS MATERIALMENTE JURISDICCIONALES. Suprema Corte de Justicia de la Nación. Tesis 2a. L/2002, Novena Época, *Semanario Judicial de la Federación y su Gaceta*, mayo de 2002, Tomo XV, p. 299.

[245] RECURSO DE RECONSIDERACIÓN PREVISTO EN EL ARTÍCULO 11 DE LA LEY DE LA

naturaleza del interés público protegido cuando sea pertinente.[246] En el caso de los órganos garantes del artículo 6° constitucional, esta adecuación lleva a la necesidad de siempre ponderar la protección de los derechos de acceso y datos personales con el interés público, a través de las pruebas de daño e interés establecidas en las correspondientes leyes generales.

De acuerdo con el análisis conceptual, podríamos definir a los recursos establecidos en la LGPDPPSO como procedimientos cuasi jurisdiccionales que son competencia de los órganos garantes y que tienen el propósito —en apego al principio de legalidad — de salvaguardar la validez de los actos de los sujetos obligados relacionados a la protección de los datos personales en su posesión, con el objeto de garantizar la eficacia de los derechos humanos relativos a la privacidad de las personas y la prerrogativa a su autodeterminación informativa. Una vez establecido el concepto jurídico procede desarrollar los elementos que los componen. Al efecto, analizaremos sus ámbitos de validez, es decir: los órganos del Estado involucrados, las autoridades competentes para conocer de los recursos, el objeto o materia de los recursos, los procedimientos, tiempo y espacio en el que es aplicable.[247]

**1. Sujetos del recurso.** Conforme al artículo 94 de la LGPDPPSO, los recursos deben ser presentados por escrito en el formato señalado por el órgano garante o en escrito libre por el particular que se ha visto afectado por un acto administrativo o por su representante legal, el cual debe estar debidamente acreditado de acuerdo con las reglas establecidas en el artículo 96 dependiendo si se trata de una persona física o moral. En el caso concreto de la LGPDPPSO, el acto consiste en la decisión u omisión de un sujeto obligado respecto de los derechos relacionados con la protección de datos personales —como los derechos ARCO de un particular. Por lo tanto, se trata de un derecho subjetivo[248] que tiene un interés jurídico dado que afecta algún

COMISIÓN REGULADORA DE ENERGÍA ABROGADA. ES INNECESARIO AGOTARLO PREVIO A PROMOVER EL JUICIO CONTENCIOSO ADMINISTRATIVO FEDERAL CONTRA EL ACUERDO GENERAL A/143/2012, DE 13 DE DICIEMBRE DE 2012, EMITIDO POR EL PLENO DE DICHO ÓRGANO, CON MOTIVO DE SU PRIMER ACTO DE APLICACIÓN. Tribunales Colegiados de Circuito. Tesis I.20o.A.7 A, Décima Época, *Semanario Judicial de la Federación y su Gaceta*, noviembre de 2016, Tomo IV, p. 2507.

[246] RECURSOS EN SEDE ADMINISTRATIVA. LOS PRINCIPIOS DE IMPARTICIÓN DE JUSTICIA, ESTABLECIDOS EN EL ARTÍCULO 17 CONSTITUCIONAL DEBEN ADECUARSE A LA NATURALEZA DE INTERÉS PÚBLICO DE AQUÉLLOS. Suprema Corte de Justicia de la Nación. Tesis 2a. LI/2002, Novena Época, *Semanario Judicial de la Federación y su Gaceta*, mayo 2002, Tomo XV, p. 303.

[247] Kelsen, H. (1989). *Teoría Pura del Derecho*. México: Porrúa.

[248] La noción de interés se encuentra íntimamente relacionada con el derecho subjetivo del gobernado. La existencia de un derecho subjetivo supone la reunión de tres elementos: Un interés exclusivo actual y directo. Éste existirá si el interés es personal, si existe al momento de promover el juicio constitucional y el bien perseguido conduce a la satisfacción de una necesidad del titular. El reconocimiento y tutela de ese interés por la ley. Es decir, la existencia de una norma jurídica creada para garantizar en forma inmediata su satisfacción. “Esto sucederá cuando de la norma surja una relación jurídica, en virtud de la cual una persona (sujeto activo) tenga el derecho de exigir la satisfacción de su interés, y otra persona (sujeto pasivo) […] tenga el deber de satisfacer

bien del gobernado (en este caso los datos personales). No sólo se trata de que el acto administrativo incida ilegalmente en su patrimonio o en su persona, sino que tiene un interés exclusivo, actual y directo. Ello otorga el derecho para que en ese procedimiento —por el que se formó el acto de autoridad— se observen las competencias y los procedimientos que la ley precisa a fin de que se respeten los principios de legalidad y seguridad jurídica.[249] Por tanto, tratándose de datos personales, es necesario acreditar el interés jurídico tal como lo señala la ley en los artículos 95 y 96 al mandatar la necesidad de acreditar que se es el titular de los derechos y establecer los medios para hacerlo. Es interesante que la LGPDPPSO en el artículo 97 señala que cuando se trata de personas fallecidas es posible interponer los recursos con el mero interés legítimo. En este último caso será importante atender a la interpretación que los órganos garantes le den a esta figura pues habría que acreditar la situación especial que tiene el demandante con respecto de los datos personales de otro individuo, por ejemplo, que es su heredero o familiar.[250]

El sujeto obligado, en estos casos, será el demandado en el recurso administrativo, quien está obligado a la satisfacción del interés mediante la prestación debida. Por ejemplo, en el caso de la LGPDPPSO, se refiere a permitir el ejercicio pleno de los derechos ARCO o a que la información entregada sea satisfactoria para el titular.

Por último, entre los sujetos se encuentra el órgano garante, quien es la autoridad competente reconocida por la ley para conocer del recurso. Además, la ley debe prever la obligación de la autoridad de dictar una resolución en cuanto al fondo determinando la validez o invalidez de la actuación de sujeto obligado. La LGPDPPSO señala que la resolución —que recae a los recursos— confirma, modifica o revoca la respuesta del sujeto obligado en el caso del recurso de revisión o del órgano garante cuando se trata de una inconformidad.

**2. El objeto de los recursos.** El objeto de los recursos o su ámbito material se refiere al acto combatido o su materia. Su finalidad, en primer lugar, radica en la revisión del acto y, de resultar procedente, la revocación, anulación o reforma del mismo. Para ello, debe existir un acto administrativo previo que sirva de causa y antecedente del recurso. Se debe de señalar un acto que lesione el derecho del gobernado porque de otra manera no existe lesión al interés jurídico, ni actuación de la autoridad. Es importante que quede claramente establecido el acto administrativo que se combate, ya que, al tener toda resolución administrativa

el interés a través de una prestación de contenido positivo, de dar o hacer, o de contenido negativo, de no hacer".

[249] Sánchez, A. (2006). *Los medios de impugnación en materia administrativa*. México: Porrúa, p. 126.

[250] INTERÉS LEGÍTIMO. SU AUSENCIA PUEDE CONSTITUIR UN MOTIVO MANIFIESTO E INDUDABLE DE IMPROCEDENCIA DEL JUICIO DE AMPARO. Suprema Corte de Justicia de la Nación. Tesis jurisprudencial 57/2017, Décima Época, *Semanario Judicial de la Federación y su Gaceta*, junio 2017, Tomo II, p. 1078.

presunción *iuris tantum* respecto a su legalidad, corresponde probar lo contrario al gobernado en su recurso.[251] En el caso de la LGPDPPSO, por ejemplo, el artículo 105 señala los requisitos que debe tener la interposición del recurso de revisión: debe constar claramente: el acto que se recurre, los puntos petitorios, las razones o motivos de la inconformidad, copia de la respuesta dada por el sujeto obligado (si la hubiere) y las pruebas que el titular considere pertinentes.

El artículo 102 señala los medios probatorios que se pueden presentar, por ejemplo: documentales, de inspección, periciales, testimoniales y confesionales. Con ellos, el titular buscará probar la invalidez de la respuesta o negativa del sujeto obligado. Sin embargo, el artículo 101 de la mencionada ley establece la posibilidad de que la presunción de validez se desvirtúe ante la negativa del sujeto obligado de responder al recurso o a los requerimientos que le haga el órgano garante, en cuyo caso, tendrá por ciertos los hechos.

**3. Los procedimientos de los recursos.** El punto de partida es que todo recurso debe estar contemplado en una ley. Esto depende del principio de legalidad y, de no existir en una ley, no se obliga a la autoridad a contrastar lo emitido con las atribuciones legales de la misma. En este caso, el título noveno de la LGPDPPSO prevé los procedimientos de impugnación para la protección de los datos personales en posesión de los sujetos obligados. Estos procedimientos determinan la autoridad competente para resolverlos cuyas facultades pueden ser la anulación o reforma del acto, reconocimiento del derecho del recurrente o el examen de la legalidad y la oportunidad del acto impugnado. Ahora bien, como apuntan Fraga y Carrillo[252] los actos administrativos siempre deben representar el interés general, de ello resulta que, al ser la impugnación de un particular, no se pueda sostener la suspensión de la ejecución del acto reclamado. Por eso mismo, la interposición del recurso no suspende, por regla general, su ejecución. El procedimiento debe seguir las formalidades del debido proceso en general: demanda, contestación, período probatorio, alegatos y resolución. En el caso de los recursos para la protección de los datos la LGPDPPSO establece tales etapas en los capítulos segundo y tercero del Título Noveno sin contemplar la suspensión de los actos emitidos por los sujetos obligados.

El artículo 102 enumera los medios probatorios que son admisibles en los recursos previstos, incluyendo los nuevos medios desarrollados por las tecnologías de la información como las páginas electrónicas. El artículo 98 señala que las notificaciones, en el procedimiento señalando, deberán ser personales en la primera notificación o cuando se haga algún requerimiento. Los plazos dentro del procedimiento comienzan a contarse al día siguiente de la notificación de acuerdo con el artículo 99. Para el pronto desahogó del

[251] Sánchez, A. (2006). *Los medios de impugnación en materia administrativa*. México: Porrúa.
[252] Carrillo, A. (1973). *La justicia Federal y la Administración Pública*. México: Porrúa.

procedimiento, como ha ordenado la SCJN, el artículo 100 señala la obligación de todo sujeto obligado y de los órganos garantes de atender los plazos establecidos en la ley.

**4. Ámbito espacial y temporal de los recursos**. Respecto del ámbito espacial de aplicación de los recursos contemplados en la LGPDPPSO, dado que se trata de una ley general, ésta es aplicable en toda la República Mexicana. Debe ser observada en materia de protección de datos personales, incluyendo la procedencia y substanciación de los recursos por los sujetos obligados del ámbito federal (incluso los órganos constitucionalmente autónomos), estatal y municipal, así como por los órganos garantes estatales y el INAI.

La LGPDPPSO entró en vigor el 27 de enero de 2017 por lo que es a partir de esta fecha que los recursos, en materia de protección de datos, son aplicables. El artículo segundo transitorio de la LGPDPPSO señala que deben ser adecuadas las leyes de transparencia federal y locales que, hasta antes de la emisión de la ley general, contemplan mecanismos de revisión respecto de datos personales en posesión de sujetos obligados.

## IV. Conclusiones

Tras el análisis de los elementos característicos de los recursos establecidos en la LGPDPPSO, es posible concluir que cumplen con las condiciones de los recursos administrativos cuasi jurisdiccionales con la doble función de, por un lado, proteger los derechos de privacidad y autodeterminación informativa de los particulares y a la vez fungir como mecanismos de control de las actuaciones de los sujetos obligados en materia de protección de datos personales. La tabla siguiente sintetiza los elementos y detalla los requisitos que deben contemplar los recursos identificando en la LGPDPPSO las disposiciones que los contemplan:

**Tabla 6. Elementos de los recursos administrativos cuasi jurisdiccionales[253]**

| Elementos de los recursos administrativos cuasi jurisdiccionales | Recursos de la LGPDPPSO |
|---|---|
| 1. La existencia de una resolución administrativa que vulnere un derecho o interés del particular | El Título Noveno de la ley establece los medios de impugnación de los actos u omisiones de todos los sujetos obligados en materia de protección de datos lo que incluye clasificación indebida de datos personales, la declaración de inexistencia, la entrega incompleta o en formatos inadecuados de los datos solicitados, la negativa u obstaculización del ejercicio de los derechos ARCO o de la entrega de la información solicitada. |
| 2. La fijación en la ley de las autoridades administrativas a quienes debe presentarse | Los órganos garantes son la autoridad competente para conocer de los medios de impugnación previstos en la ley. Cuando se trata de sujetos obligados federales o nacionales, o la revisión de las resoluciones de los órganos garantes locales será el INAI y cuando se trata de los sujetos obligados locales o municipales será el órgano garante de la entidad federativa correspondiente. |
| 3. La fijación de un plazo para la interposición del recurso | Tanto en el recurso de revisión como en el de inconformidad el plazo para su interposición es de 15 días a partir de que el particular reciba la respuesta o resolución, o en su defecto, que haya vencido el plazo para interponerlo. |
| 4. Los requisitos de forma y elementos que deben incluirse en el escrito de interposición del recurso | El artículo 94 establece que los recursos se interpondrán ante el órgano garante o la unidad de transparencia correspondiente y puede hacerse por escrito libre, por correo certificado, mediante los formatos emitidos por el órgano garante, por medios electrónicos.<br>El artículo 105 establece los elementos que debe contener el escrito de interposición del recurso: área responsable, nombre del recurrente, fecha de notificación de la respuesta impugnada, acto que se impugna y pruebas. |
| 5. La fijación de un procedimiento para la tramitación del recurso | El titulo noveno establece procedimientos diferenciados en sus capítulos segundo y tercero para la substanciación de los recursos mismos que se analizan a detalle más adelante. |
| 6. La obligación de la autoridad revisora de dictar nueva resolución | Tal obligación y las modalidades que debe contemplar se detallan en los capítulos segundo y tercero del Título Noveno. |

[253] Enlistadas en Fraga, G. (2000). *Derecho administrativo*. México: Porrúa.

## Referencias

Cámara de Diputados. (2015). *Dictamen de las Comisiones Unidas de Gobernación y de Estudios Legislativos Primera, con proyecto de decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*. p. 57. [Archivo PDF]. Disponible en: http://www.senado.gob.mx/comisiones/gobernacion/docs/proteccion_datos/Documento3.pdf, [fecha de consulta: 7 de mayo 2018].

Carrillo, A. (1973). *La justicia Federal y la Administración Pública*. México: Porrúa.

DOF. (2016). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, *Diario Oficial de la Federación*.

Fernández, J. (2005). *Derecho administrativo y administración pública*. México: UNAM, Porrúa.

Fierro, A. (2017). *El Sistema Normativo de Rendición de Cuentas y el Ciclo del Uso de los Recursos Públicos en el Orden Jurídico Mexicano* (Tesis doctoral). México: Instituto de Investigaciones Jurídicas de la UNAM.

Fraga, G. (2000). *Derecho administrativo*. México: Porrúa.

García de Enterría, E. y Fernández, T. (2011). *Curso de derecho administrativo*, Tomo II. España: Thompson Reuters.

Kelsen, H. (1989). *Teoría Pura del Derecho*. México: Porrúa.

Sánchez, A. (2006). *Los medios de impugnación en materia administrativa*. México: Porrúa.

Senado de la República. (2016). *Pre-Proyecto de Dictamen de las Comisiones Unidas de Gobernación y de Estudios Legislativos Primera, con Proyecto de Decreto por el que se expide la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*. [Archivo PDF]. Disponible en: http://www.senado.gob.mx/comisiones/gobernacion/docs/proteccion_datos/Documento3.pdf, [fecha de consulta: 7 de mayo 2018].

Suprema Corte de Justicia de la Nación. (mayo 2002). Tesis 2a. L/2002, Novena Época, *Semanario Judicial de la Federación y su Gaceta*. Tomo XV, p. 299.

Suprema Corte de Justicia de la Nación. (mayo 2002). Tesis 2a. LI/2002, Novena Época, *Semanario Judicial de la Federación y su Gaceta*. Tomo XV, p. 303.

Suprema Corte de Justicia de la Nación. (febrero 2016). Tesis XXII.1o.1 CS, Décima Época, *Semanario Judicial de la Federación y su Gaceta*. Tomo III, p. 2060.

Suprema Corte de Justicia de la Nación. (junio 2017). Tesis jurisprudencial 57/2017, Décima Época, *Semanario Judicial de la Federación y su Gaceta*. Tomo II, p. 1078.

Tribunales Colegiados de Circuito. (octubre 2007). Tesis I.13o.A.142 A, Novena Época, *Semanario Judicial de la Federación y su Gaceta*. Tomo XXVI. p. 3349.

Tribunales Colegiados de Circuito. (julio 2015). Tesis 2o.A.E.20 A, Décima Época, *Semanario Judicial de la Federación y su Gaceta*. Libro 20, Tomo II. p. 755.

Tribunales Colegiados de Circuito. (noviembre 2016). Tesis I.20o.A.7 A, Décima Época, *Semanario Judicial de la Federación y su Gaceta*. Tomo IV, p. 2507.

Tribunales Colegiados de Circuito. (febrero de 2017). Tesis I.2o.A.E.1 CS, Décima Época, *Semanario Judicial de la Federación y su Gaceta*. Libro 39, p. 2364.

Tribunales Colegiados de Circuito. (agosto de 2017). Tesis XVI.1o.A.135 A, Décima Época, *Semanario Judicial de la Federación y su Gaceta*. Libro 45. Tomo IV, p. 2928.

# CAPÍTULO II
# DEL RECURSO DE REVISIÓN ANTE EL INSTITUTO Y LOS ORGANISMOS GARANTES

***Artículo 103.*** *El titular, por sí mismo o a través de su representante, podrá interponer un recurso de revisión ante el Instituto o, en su caso, ante los Organismos garantes o la Unidad de Transparencia del responsable que haya conocido de la solicitud para el ejercicio de los derechos ARCO, dentro de un plazo que no podrá exceder de quince días contados a partir del siguiente a la fecha de la notificación de la respuesta.*

*Transcurrido el plazo previsto para dar respuesta a una solicitud para el ejercicio de los derechos ARCO sin que se haya emitido ésta, el titular o, en su caso, su representante podrán interponer el recurso de revisión dentro de los quince días siguientes al que haya vencido el plazo para dar respuesta.*

***Artículo 104.*** *El recurso de revisión procederá en los siguientes supuestos:*

*I. Se clasifiquen como confidenciales los datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables;*

*II. Se declare la inexistencia de los datos personales;*

*III. Se declare la incompetencia por el responsable;*

*IV. Se entreguen datos personales incompletos;*

*V. Se entreguen datos personales que no correspondan con lo solicitado;*

*VI. Se niegue el acceso, rectificación, cancelación u oposición de datos personales;*

*VII. No se dé respuesta a una solicitud para el ejercicio de los derechos ARCO dentro de los plazos establecidos en la presente Ley y demás disposiciones que resulten aplicables en la materia;*

*VIII. Se entregue o ponga a disposición datos personales en una modalidad o formato distinto al solicitado, o en un formato incomprensible;*

*IX. El titular se inconforme con los costos de reproducción, envío o tiempos de entrega de los datos personales;*

*X. Se obstaculice el ejercicio de los derechos ARCO, a pesar de que fue notificada la procedencia de los mismos;*

*XI. No se dé trámite a una solicitud para el ejercicio de los derechos ARCO, y*

*XII. En los demás casos que dispongan las leyes.*

***Artículo 105.*** *Los únicos requisitos exigibles en el escrito de interposición del recurso de revisión serán los siguientes:*

*I. El área responsable ante quien se presentó la solicitud para el ejercicio de los derechos ARCO;*

*II. El nombre del titular que recurre o su representante y, en su caso, del tercero interesado, así como el domicilio o medio que señale para recibir notificaciones;*

*III. La fecha en que fue notificada la respuesta al titular, o bien, en caso de falta de respuesta la fecha de la presentación de la solicitud para el ejercicio de los derechos ARCO;*

*IV. El acto que se recurre y los puntos petitorios, así como las razones o motivos de inconformidad;*

*V. En su caso, copia de la respuesta que se impugna y de la notificación correspondiente, y*

*VI. Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante.*

*Al recurso de revisión se podrán acompañar las pruebas y demás elementos que considere el titular procedentes someter a juicio del Instituto o, en su caso, de los Organismos garantes.*

*En ningún caso será necesario que el titular ratifique el recurso de revisión interpuesto.*

***Artículo 106.*** *Una vez admitido el recurso de revisión, el Instituto o, en su caso, los Organismos garantes podrán buscar una conciliación entre el titular y el responsable.*

*De llegar a un acuerdo, éste se hará constar por escrito y tendrá efectos vinculantes. El recurso de revisión quedará sin materia y el Instituto, o en su caso, los Organismos garantes, deberán verificar el cumplimiento del acuerdo respectivo.*

***Artículo 107.*** *Admitido el recurso de revisión y sin perjuicio de lo dispuesto por el artículo 65 de la presente Ley, el Instituto promoverá la conciliación entre las partes, de conformidad con el siguiente procedimiento:*

*I. El Instituto y los Organismos garantes, según corresponda, requerirán a las partes que manifiesten, por cualquier medio, su voluntad de conciliar, en un plazo no mayor a siete días, contados a partir de la notificación de dicho acuerdo, mismo que contendrá un resumen del recurso de revisión y de la respuesta del responsable si la hubiere, señalando los elementos comunes y los puntos de controversia.*

*La conciliación podrá celebrarse presencialmente, por medios remotos o locales de comunicación electrónica o por cualquier otro medio que determine el Instituto o los Organismos garantes, según corresponda. En cualquier caso, la conciliación habrá de hacerse constar por el medio que permita acreditar su existencia.*

*Queda exceptuado de la etapa de conciliación, cuando el titular sea menor de edad y se haya vulnerado alguno de los derechos contemplados en la Ley para la Protección de los Derechos de Niñas, Niños y Adolescentes, vinculados con la ley y el reglamento, salvo que cuente con representación legal debidamente acreditada;*

*II. Aceptada la posibilidad de conciliar por ambas partes, el Instituto y los Organismos garantes, según correspondan, señalarán el lugar o medio, día y hora para la celebración de una audiencia de conciliación, la cual deberá realizarse dentro de los diez días siguientes en que el Instituto o los Organismos garantes, según corresponda, hayan recibido la manifestación de la voluntad de conciliar de ambas partes, en la que se procurará avenir los intereses entre el titular y el responsable.*

*El conciliador podrá, en todo momento en la etapa de conciliación, requerir a las partes que presenten en un plazo máximo de cinco días, los elementos de convicción que estime necesarios para la conciliación.*

*El conciliador podrá suspender cuando lo estime pertinente o a instancia de ambas partes la audiencia por una ocasión. En caso de que se suspenda la audiencia, el conciliador señalará día y hora para su reanudación dentro de los cinco días siguientes.*

*De toda audiencia de conciliación se levantará el acta respectiva, en la que conste el resultado de la misma. En caso de que el responsable o el titular o sus respectivos representantes no firmen el acta, ello no afectará su validez, debiéndose hacer constar dicha negativa;*

*III. Si alguna de las partes no acude a la audiencia de conciliación y justifica su ausencia en un plazo de tres días, será convocado a una segunda audiencia de conciliación, en el plazo de cinco días; en caso de que no acuda a esta última, se continuará con el recurso de revisión. Cuando alguna de las partes no acuda a la audiencia de conciliación sin justificación alguna, se continuará con el procedimiento;*

*IV. De no existir acuerdo en la audiencia de conciliación, se continuará con el recurso de revisión;*

*V. De llegar a un acuerdo, éste se hará constar por escrito y tendrá efectos vinculantes. El recurso de revisión quedará sin materia y el Instituto, o en su caso, los Organismos garantes, deberán verificar el cumplimiento del acuerdo respectivo, y*

*VI. El cumplimiento del acuerdo dará por concluido la sustanciación del recurso de revisión, en caso contrario, el Instituto reanudará el procedimiento.*

*El plazo al que se refiere el artículo siguiente de la presente Ley será suspendido durante el periodo de cumplimiento del acuerdo de conciliación.*

***Artículo 108.*** *El Instituto y los Organismos garantes resolverán el recurso de revisión en un plazo que no podrá exceder de cuarenta días, el cual podrá ampliarse hasta por veinte días por una sola vez.*

***Artículo 109.*** *Durante el procedimiento a que se refiere el presente Capítulo, el Instituto y los Organismos garantes, según corresponda, deberán aplicar la suplencia de la queja a favor del titular, siempre y cuando no altere el contenido original del recurso de revisión, ni modifique los hechos o peticiones expuestas en el mismo, así como garantizar que las partes puedan presentar los argumentos y constancias que funden y motiven sus pretensiones.*

***Artículo 110.*** *Si en el escrito de interposición del recurso de revisión el titular no cumple con alguno de los requisitos previstos en el artículo 105 de la presente Ley y el Instituto y los Organismos garantes, según corresponda, no cuenten con elementos para subsanarlos, éstos deberán requerir al titular, por una sola ocasión, la información que subsane las omisiones en un plazo que no podrá exceder de cinco días, contados a partir del día siguiente de la presentación del escrito.*

*El titular contará con un plazo que no podrá exceder de cinco días, contados a partir del día siguiente al de la notificación de la prevención, para subsanar las omisiones, con el apercibimiento de que en caso de no cumplir con el requerimiento, se desechará el recurso de revisión.*

*La prevención tendrá el efecto de interrumpir el plazo que tienen el Instituto y los organismos garantes para resolver el recurso, por lo que comenzará a computarse a partir del día siguiente a su desahogo.*

***Artículo 111.*** *Las resoluciones del Instituto o, en su caso, de los Organismos garantes podrán:*

*I. Sobreseer o desechar el recurso de revisión por improcedente;*

*II. Confirmar la respuesta del responsable;*

*III. Revocar o modificar la respuesta del responsable, o*

*IV. Ordenar la entrega de los datos personales, en caso de omisión del responsable.*

*Las resoluciones establecerán, en su caso, los plazos y términos para su cumplimiento y los procedimientos para asegurar su ejecución. Los responsables deberán informar al Instituto o, en su caso, a los Organismos garantes el cumplimiento de sus resoluciones.*

*Ante la falta de resolución por parte del Instituto, o en su caso, de los Organismos garantes, se entenderá confirmada la respuesta del responsable.*

*Cuando el Instituto, o en su caso, los Organismos garantes, determinen durante la sustanciación del recurso de revisión que se pudo haber incurrido en una probable responsabilidad por el incumplimiento a las obligaciones previstas en la presente Ley y demás disposiciones que resulten aplicables en la materia, deberán hacerlo del conocimiento del órgano interno de control o de la instancia competente para que ésta inicie, en su caso, el procedimiento de responsabilidad respectivo.*

***Artículo 112.*** *El recurso de revisión podrá ser desechado por improcedente cuando:*

*I. Sea extemporáneo por haber transcurrido el plazo establecido en el artículo 103 de la presente Ley;*

*II. El titular o su representante no acrediten debidamente su identidad y personalidad de este último;*

*III. El Instituto o, en su caso, los Organismos garantes hayan resuelto anteriormente en definitiva sobre la materia del mismo;*

*IV. No se actualice alguna de las causales del recurso de revisión previstas en el artículo 104 de la presente Ley;*

*V. Se esté tramitando ante los tribunales competentes algún recurso o medio de defensa interpuesto por el recurrente, o en su caso, por el*

*tercero interesado, en contra del acto recurrido ante el Instituto o los Organismos garantes, según corresponda;*

*VI. El recurrente modifique o amplíe su petición en el recurso de revisión, únicamente respecto de los nuevos contenidos, o*

*VII. El recurrente no acredite interés jurídico.*

*El desechamiento no implica la preclusión del derecho del titular para interponer ante el Instituto o los Organismos garantes, según corresponda, un nuevo recurso de revisión.*

***Artículo 113.*** *El recurso de revisión solo podrá ser sobreseído cuando:*

*I. El recurrente se desista expresamente;*

*II. El recurrente fallezca;*

*III. Admitido el recurso de revisión, se actualice alguna causal de improcedencia en los términos de la presente Ley;*

*IV. El responsable modifique o revoque su respuesta de tal manera que el recurso de revisión quede sin materia, o*

*V. Quede sin materia el recurso de revisión.*

***Artículo 114.*** *El Instituto y los Organismos garantes deberán notificar a las partes y publicar las resoluciones, en versión pública, a más tardar, al tercer día siguiente de su aprobación.*

***Artículo 115.*** *Las resoluciones del Instituto y de los Organismos garantes serán vinculantes, definitivas e inatacables para los responsables.*

*Los titulares podrán impugnar dichas resoluciones ante el Poder Judicial de la Federación mediante el Juicio de Amparo.*

***Artículo 116.*** *Tratándose de las resoluciones a los recursos de revisión de los Organismos garantes de las Entidades Federativas, los particulares podrán optar por acudir ante el Instituto interponiendo el recurso de inconformidad previsto en esta Ley o ante el Poder Judicial de la Federación mediante el Juicio de Amparo.*

# COMENTARIO

**Ana Elena Fierro**

## I. Antecedentes

El capítulo segundo del Título Noveno de la LGPDPPSO establece al recurso de revisión como el medio de impugnación de las actuaciones en materia de protección de datos personales en posesión de los sujetos obligados. Como quedó señalado en el capítulo anterior se trata de un recurso administrativo cuasi jurisdiccional en virtud de que las autoridades competentes para resolverlo son distintas del órgano que las emitió a través de un procedimiento en forma de juicio. Se trata de los órganos garantes, tanto nacional como de las entidades federativas, que conforme con la Constitución tienen entre sus objetivos garantizar la eficacia de los derechos humanos relativos a la privacidad de las personas y la prerrogativa a su autodeterminación informativa. El recurso de revisión, además, permite salvaguardar la validez de los actos de los sujetos obligados relativos a la protección de los datos personales constituyéndose en un mecanismo de rendición de cuentas.

## II. Relevancia temática y contexto

El recurso de revisión permite la salvaguarda del principio de legalidad que rige a toda actuación de los órganos de Estado, pues implica que el particular tiene derecho a que cualquier autoridad, al momento de actuar, cumpla con los siguientes requisitos: que tenga competencia para hacerlo y que se apegue a las formalidades, motivo, objeto y fin prescritos por la ley.[254] En el caso concreto de la LGPDPPSO el recurso de revisión previsto tiene por objeto garantizar el efectivo ejercicio de los derechos ARCO, concediendo, a los particulares, un medio para defenderse ante negativas u omisiones en el ejercicio de los derechos relacionados con sus datos personales. Los elementos que componen al recurso de revisión se esquematizan a partir de sus ámbitos de validez normativa en la tabla siguiente:

[254] Fraga, G. (2000). *Derecho administrativo*. México: Porrúa.

**Tabla 7. Análisis del recurso de revisión de la LGPDPPSO**

| Elementos de los recursos administrativos | LGPDPPSO, Título Noveno capítulo II del Recurso de revisión ante el Instituto y los organismos garantes[255] |
|---|---|
| Sujetos | **Demandante:** el titular de los datos personales o su representante debidamente acreditado ante la negativa de entregar los datos, ser omiso en la respuesta o entregarlos incompletos por parte del sujeto obligado (artículo 103).<br>**Demandado:** sujeto obligado en posesión de los datos personales debe establecerse el área responsable ante quien se presentó la solicitud (artículo 105, I).<br>**Autoridad:** El Instituto conocerá del recurso cuando el demandado sea un sujeto obligado federal y corresponde a los organismos si se trata de un sujeto obligado de carácter local. Es posible presentar el recurso ante la Unidad de Transparencia del sujeto obligado o a través de los medios electrónicos previstos por la ley (artículos 94 y 103). |
| Objeto o materia del recurso | Conforme al artículo 104, el recurso procede cuando:<br>I. Se clasifiquen como confidenciales los datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables.<br>II. Se declare la inexistencia de los datos personales.<br>III. Se declare la incompetencia por el responsable.<br>IV. Se entreguen datos personales incompletos.<br>V. Se entreguen datos personales que no correspondan con lo solicitado.<br>VI. Se niegue el acceso, rectificación, cancelación u oposición de datos personales.<br>VII. No se dé respuesta a una solicitud para el ejercicio de los derechos ARCO dentro de los plazos establecidos en la presente Ley y demás disposiciones que resulten aplicables en la materia.<br>VIII. Se entregue o ponga a disposición datos personales en una modalidad o formato distinto al solicitado o en un formato incomprensible.<br>IX. El titular se inconforme con los costos de reproducción, envío o tiempos de entrega de los datos personales.<br>X. Se obstaculice el ejercicio de los derechos ARCO, a pesar de que fue notificada la procedencia de los mismos.<br>XI. No se dé trámite a una solicitud para el ejercicio de los derechos ARCO.<br>XII. En los demás casos que dispongan las leyes. |

[255] Conforme al artículo 3 de la LGPDPPSO, se distinguen a los órganos garantes denominando *Instituto* al órgano garante nacional (esto es, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales) y *organismos* a los órganos con autonomía constitucional especializados en materia de acceso a la información y protección de datos personales conforme a los artículos 6º y 116, VIII de la Constitución.

| Elementos de los recursos administrativos | LGPDPPSO, Título Noveno capítulo II del Recurso de revisión ante el Instituto y los organismos garantes |
|---|---|
| Competencia de los órganos garantes para conocer del recurso | **INAI**: cuando se trata de datos personales en posesión de sujetos obligados federales incluyendo otros órganos constitucionales autónomos o cuando se trate de un recurso de revisión que, por su interés y trascendencia, ameriten que se ejerza la facultad de atracción (artículo 130).<br>**Organismos garantes**: cuando se trata de datos personales en posesión de sujetos obligados locales o municipales. |
| Procedimiento cuasi jurisdiccional | 1. Recibida la demanda el órgano garante debe requerir a los sujetos obligados la contestación a la demanda y toda la información necesaria para estar en condiciones de resolver el recurso.<br>2. Recibir y desahogar las pruebas establecidas en el artículo 102.<br>3. El órgano garante tiene la facultad de suplir la queja a favor del titular cuando fuese necesario, es decir, puede completar o corregir las deficiencias del escrito del recurso. Además, lo puede solicitar para que aclare su escrito en un plazo de cinco días de lo contrario desecha el recurso (artículos 109 y 110). También será desechado por improcedente el recurso cuando (artículo112):<br>I. Sea extemporáneo por haber transcurrido el plazo establecido en el artículo 103 de la presente Ley.<br>II. El titular o su representante no acrediten debidamente su identidad y personalidad de este último.<br>III. El Instituto o, en su caso, los organismos garantes hayan resuelto anteriormente en definitiva sobre la materia del mismo.<br>IV. No se actualice alguna de las causales del recurso de revisión previstas en el artículo 104 de la Ley.<br>V. Se esté tramitando ante los tribunales competentes algún recurso o medio de defensa interpuesto por el recurrente, o en su caso, por el tercero interesado en contra del acto recurrido ante el Instituto o los organismos garantes, según corresponda.<br>VI. El recurrente modifique o amplíe su petición en el recurso de revisión, únicamente respecto de los nuevos contenidos.<br>VII. El recurrente no acredite interés jurídico.<br>4. El órgano garante cuenta con 40 días para resolver y puede ampliarse 20 más (artículo 108). A falta de resolución se entenderá confirmada la respuesta del sujeto obligado pudiendo el titular acudir al recurso de inconformidad tratándose de sujetos obligados locales o al juicio de amparo (artículos 111, 116). |

Tabla 7. Continúa

| Elementos de los recursos administrativos | LGPDPPSO, Título Noveno capítulo II del Recurso de revisión ante el Instituto y los organismos garantes |
|---|---|
| Propósito:<br>Sentido de la Resolución | Las resoluciones de los órganos garantes tienen por objeto determinar si la respuesta del sujeto obligado es correcta y confirmarla o bien debe ser corregida o vuelta a hacer por completo a fin de garantizar los derechos ARCO. El sentido de la resolución puede tener las siguientes consecuencias:<br>I. Sobreseer o desechar el recurso de revisión por improcedente; es decir por estar incompleta o adolecer de los requisitos de presentación señalados en la ley. Las causas de sobreseimiento están previstas en el artículo 113 y se refieren al desistimiento o muerte de quien promueve, la modificación o revocación de la respuesta impugnada o porque quede sin materia el recurso.<br>II. Confirmar la respuesta del responsable, es decir, señalar que la respuesta del sujeto obligado fue correcta.<br>III. Revocar o modificar la respuesta del responsable, es decir, señalar que la respuesta es totalmente incorrecta y debe emitir una nueva en el sentido correcto o bien que es parcialmente incorrecta y por lo tanto debe hacer las correcciones que la resolución indique.<br>IV. Ordenar la entrega de los datos personales en caso de omisión del responsable.<br>Las resoluciones establecerán, en su caso, los plazos y términos para su cumplimiento y los procedimientos para asegurar su ejecución. Los responsables deberán informar a los órganos garantes el cumplimiento de sus resoluciones (artículo 111). Las resoluciones de los órganos garantes deben notificarse a las partes y ser publicadas en versión pública (artículo 114).<br>Las resoluciones del recurso de revisión son definitivas e inatacables para los sujetos obligados (artículo 115), es decir, deben darles cumplimiento en cuanto les son notificadas. Los particulares pueden, si no están de acuerdo con la resolución, interponer el recurso de inconformidad ante el INAI o promover un juicio de amparo (artículo 116), con ello se busca dotar al particular de todos los medios para la adecuada defensa de sus derechos ante posibles errores u omisiones de los órganos garantes. |

## III. Análisis del contenido

El recurso de revisión previsto en la LGPDPPSO tiene un carácter cuasi jurisdiccional enfocado en hacer efectivos los derechos de protección de datos personales, de ahí que otorgue facultades a los órganos garantes para suplir las deficiencias en el escrito del titular o solicitar que subsane las omisiones, además de tener las facultades de dar por cierto los hechos materia del procedimiento, si el sujeto obligado fuera omiso a los requerimientos que le

formule en la substanciación del recurso. La resolución conforme al artículo 111 debe señalar con claridad todas las condiciones para su debido cumplimiento.

Adicionalmente, la ley otorga a los órganos garantes medidas de apremio para asegurar la ejecución cabal de sus resoluciones (artículos 152 a 162). De modo que los órganos garantes cuenten con las herramientas para poder dictar las resoluciones y asegurar su cumplimiento, garantizando con ello el ejercicio de los derechos ARCO. Asimismo, la ley faculta a los órganos garantes para denunciar, ante los órganos internos de control correspondientes, la probable responsabilidad de los servidores públicos dentro del sujeto obligado por el incumplimiento a las obligaciones previstas en la LGPDPPSO y demás disposiciones que resulten aplicables en la materia (artículo 111).

Ahora bien, el recurso de revisión también posee el carácter de corrección de las actuaciones de los sujetos obligados no sólo en virtud de que deben cumplir con la resolución, sino también porque la propia ley otorga al órgano garante la competencia para promover una conciliación entre las partes. Además, el artículo 114 ordena la publicación de versiones públicas de las resoluciones con lo que se refuerza el carácter pedagógico que puede darse a las mismas, pues tanto los sujetos obligados como todas las personas pueden conocer los criterios y argumentos emitidos por el órgano garante. Estas herramientas de conciliación, medidas de apremio, prevenciones y publicidad de las resoluciones muestran este doble carácter del recurso como garante de derechos y como mecanismo de rendición de cuentas para el control de la actuación de los sujetos obligados. Asimismo, el recurso de inconformidad o la posibilidad de interponer un amparo permite a los ciudadanos contar con un medio de control de la actuación de los órganos garantes, pues las resoluciones que emitieron en el recurso de revisión serán a su vez analizadas o por el INAI o por el Poder Judicial de la Federación, respectivamente.

Los artículos 106 y 107 de la LGPDPPSO establecen el procedimiento de conciliación que, una vez admitido el recurso de revisión, el órgano garante puede promover. Se trata de un medio alternativo de solución de controversias que tiene por objeto primordial buscar de manera voluntaria, flexible y por mutuo acuerdo de las partes la solución del conflicto planteado.[256] La conciliación, a diferencia del medio de impugnación que busca determinar la validez o no de la actuación del sujeto obligado, se enfoca en lograr una solución mediante el diálogo entre las partes. Para ello se celebran audiencias donde se levanta un acta y si se llega a un acuerdo, éste se hace constar por escrito con efectos vinculantes para ambos. Además, se establece el deber del órgano garante de dar seguimiento al cumplimiento del acuerdo. Si el sujeto obligado incumpliera el acuerdo, el órgano garante podrá reanudar la substanciación del recurso de

[256] Fierro, A. (2010). *Manejo de Conflictos y Mediación*. México: CIDE/Oxford.

revisión. Luego, la posibilidad de acudir a una conciliación entre el titular y el sujeto obligado parece atender a la finalidad apuntada en el capítulo anterior relativo a que uno de los objetivos de los recursos es que la administración tenga la oportunidad de corregir errores u omisiones. En este sentido, resulta que el recurso también se constituye en un medio de rendición de cuentas[257] que, además de garantizar el efectivo ejercicio de los derechos de protección de datos, busca la mejora en la actuación de los sujetos obligados respecto del manejo de los datos personales que poseen, a través de un diálogo entre el particular afectado y el sujeto obligado. Lo anterior, de hecho, va en línea con la misión de los órganos garantes como protectores de los derechos relacionados con los datos personales y la autodeterminación informativa de todas las personas.

## IV. Conclusiones

La LGPDPPSO contempla la existencia de un conjunto de recursos que hemos definido como cuasi jurisdiccionales, los cuales tienen la doble finalidad de, por un lado, constituir herramientas para garantizar el eficaz cumplimiento de los derechos de protección de datos personales y autodeterminación informativa de todas las personas y a la vez, conforman un medio de control de la actuación de los sujetos obligados que les permite la corrección de sus errores u omisiones en el tratamiento de los datos personales que poseen. Con ello permiten, además, que los órganos garantes cuenten con procedimientos de rendición de cuentas para el cumplimiento de sus obligaciones como garantes de los derechos establecidos en el artículo 6° constitucional. Este segundo propósito resulta evidente dada la posibilidad establecida en ley de resolver el conflicto mediante una conciliación donde el énfasis no es ya la validez o invalidez de la actuación del sujeto obligado, sino la solución al conflicto planteado, de modo que el titular ejerza el pleno ejercicio de sus derechos ARCO, además de la publicidad de las resoluciones que permite hacer del conocimiento público los criterios de corrección emitidos por el órgano garante.

Por otro lado, es importante no perder de vista que estos recursos deben ser accesibles, sencillos y expeditos, para ello, la LGPDPPSO dota a los órganos garantes de diversos medios como el uso de las tecnologías de la información o las medidas de apremio, de modo que realmente están en posibilidades de garantizar el eficaz ejercicio de los derechos que la Constitución les ha encomendado y esperamos que así sea.

[257] Se entiende por rendición de cuentas el procedimiento mediante el cual una autoridad explica y justifica su actuación (en este caso la respuesta del sujeto obligado) a otra autoridad facultada para analizarla, determinar su validez y sancionar (en este caso el órgano garante quien dicta la resolución mediante la que confirma, modifica o revoca la respuesta recurrida) Fierro, A. (2017). *El Sistema Normativo de Rendición de Cuentas y el Ciclo del Uso de los Recursos Públicos en el Orden Jurídico Mexicano* (Tesis doctoral). México: Instituto de Investigaciones Jurídicas de la UNAM.

## Referencias

DOF. (2014). Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, *Diario Oficial de la Federación*.

DOF. (2017). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, *Diario Oficial de la Federación*.

Fierro, A. (2010). *Manejo de Conflictos y Mediación*. México: Centro de Investigación y Docencia Económicas/Oxford.

Fierro, A. (2017). *El Sistema Normativo de Rendición de Cuentas y el Ciclo del Uso de los Recursos Públicos en el Orden Jurídico Mexicano* (Tesis doctoral). México: Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México.

Fraga, G. (2000). *Derecho administrativo*. México: Porrúa.

# CAPÍTULO III
# DEL RECURSO DE INCONFORMIDAD ANTE EL INSTITUTO

***Artículo 117.*** *El titular, por sí mismo o a través de su representante, podrá impugnar la resolución del recurso de revisión emitido por el organismo garante ante el Instituto, mediante el recurso de inconformidad.*

*El recurso de inconformidad se podrá presentar ante el organismo garante que haya emitido la resolución o ante el Instituto, dentro de un plazo de quince días contados a partir del siguiente a la fecha de la notificación de la resolución impugnada.*

*Los Organismos garantes deberán remitir el recurso de inconformidad al Instituto al día siguiente de haberlo recibido; así como las constancias que integren el procedimiento que haya dado origen a la resolución impugnada, el cual resolverá allegándose de los elementos que estime convenientes.*

***Artículo 118.*** *El recurso de inconformidad procederá contra las resoluciones emitidas por los Organismos garantes de las Entidades Federativas que:*

*I. Clasifiquen los datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables;*

*II. Determinen la inexistencia de datos personales, o*

*III. Declaren la negativa de datos personales, es decir:*

*a) Se entreguen datos personales incompletos;*

*b) Se entreguen datos personales que no correspondan con los solicitados;*

*c) Se niegue el acceso, rectificación, cancelación u oposición de datos personales;*

*d) Se entregue o ponga a disposición datos personales en un formato incomprensible;*

*e) El titular se inconforme con los costos de reproducción, envío, o tiempos de entrega de los datos personales, o*

*f) Se oriente a un trámite específico que contravenga lo dispuesto por el artículo 54 de la presente Ley.*

***Artículo 119.*** *Los únicos requisitos exigibles e indispensables en el escrito de interposición del recurso de inconformidad son:*

*I. El área responsable ante la cual se presentó la solicitud para el ejercicio de los derechos ARCO;*

*II. El organismo garante que emitió la resolución impugnada;*

*III. El nombre del titular que recurre o de su representante y, en su caso, del tercero interesado, así como su domicilio o el medio que señale para recibir notificaciones;*

*IV. La fecha en que fue notificada la resolución al titular;*

*V. El acto que se recurre y los puntos petitorios, así como las razones o motivos de inconformidad;*

*VI. En su caso, copia de la resolución que se impugna y de la notificación correspondiente, y*

*VII. Los documentos que acrediten la identidad del titular y, en su caso, la personalidad e identidad de su representante.*

*El promovente podrá acompañar su escrito con las pruebas y demás elementos que considere procedentes someter a juicio del Instituto.*

***Artículo 120.*** *El Instituto resolverá el recurso de inconformidad en un plazo que no podrá exceder de treinta días contados a partir del día siguiente de la interposición del recurso de inconformidad, plazo que podrá ampliarse por una sola vez y hasta por un periodo igual.*

***Artículo 121.*** *Durante el procedimiento a que se refiere el presente Capítulo, el Instituto deberá aplicar la suplencia de la queja a favor del titular, siempre y cuando no altere el contenido original del recurso de inconformidad, ni modifique los hechos o peticiones expuestas en el mismo, así como garantizar que las partes puedan presentar los argumentos y constancias que funden y motiven sus pretensiones.*

***Artículo 122.*** *Si en el escrito de interposición del recurso de inconformidad el titular no cumple con alguno de los requisitos previstos en el artículo 119 de la presente Ley y el Instituto no cuente con elementos para subsanarlos, éste deberá requerir al titular, por una sola ocasión, la información que subsane las omisiones en un plazo que no podrá exceder de cinco días, contados a partir del día siguiente de la presentación del escrito.*

*El titular contará con un plazo que no podrá exceder de quince días, contados a partir del día siguiente al de la notificación de la prevención, para subsanar las omisiones, con el apercibimiento de que en caso de no cumplir con el requerimiento, se desechará el recurso de inconformidad.*

*La prevención tendrá el efecto de interrumpir el plazo que tiene el Instituto para resolver el recurso, por lo que comenzará a computarse a partir del día siguiente a su desahogo.*

***Artículo 123.*** *Una vez concluida la etapa probatoria, el Instituto pondrá a disposición de las partes las actuaciones del procedimiento y les otorgará un plazo de cinco días para que formulen alegatos contados a partir de la notificación del acuerdo a que se refiere este artículo.*

***Artículo 124.*** *Las resoluciones del Instituto podrán:*

*I. Sobreseer o desechar el recurso de inconformidad;*

*II. Confirmar la resolución del organismo garante;*

*III. Revocar o modificar la resolución del organismo garante, o*

*IV. Ordenar la entrega de los datos personales, en caso de omisión del responsable.*

*Las resoluciones establecerán, en su caso, los plazos y términos para su cumplimiento y los procedimientos para asegurar su ejecución. Los Organismos garantes deberán informar al Instituto sobre el cumplimiento de sus resoluciones.*

*Si el Instituto no resuelve dentro del plazo establecido en este Capítulo, la resolución que se recurrió se entenderá confirmada.*

*Cuando el Instituto determine durante la sustanciación del recurso de inconformidad, que se pudo haber incurrido en una probable responsabilidad por el incumplimiento a las obligaciones previstas en la presente Ley y a las demás disposiciones aplicables en la materia, deberá hacerlo del conocimiento del órgano interno de control o de la instancia competente para que ésta inicie, en su caso, el procedimiento de responsabilidad respectivo.*

*Las medidas de apremio previstas en la presente Ley, resultarán aplicables para efectos del cumplimiento de las resoluciones que recaigan a los recursos de inconformidad. Estas medidas de apremio deberán establecerse en la propia resolución.*

***Artículo 125.*** *El recurso de inconformidad podrá ser desechado por improcedente cuando:*

*I. Sea extemporáneo por haber transcurrido el plazo establecido en el artículo 117 de la presente Ley;*

*II. El Instituto anteriormente haya resuelto en definitiva sobre la materia del mismo;*

*III. No se actualicen las causales de procedencia del recurso de inconformidad, previstas en el artículo 118 de la presente Ley;*

*IV. Se esté tramitando ante el Poder Judicial algún recurso o medio de defensa interpuesto por el titular, o en su caso, por el tercero interesado, en contra del acto recurrido, o*

*V. El inconforme amplíe su solicitud en el recurso de inconformidad, únicamente respecto de los nuevos contenidos.*

***Artículo 126.*** *El recurso de inconformidad solo podrá ser sobreseído cuando:*

*I. El recurrente se desista expresamente;*

*II. El recurrente fallezca;*

*III. El organismo garante modifique o revoque su respuesta de tal manera que el recurso de inconformidad quede sin materia, o*

*IV. Admitido el recurso, se actualice alguna causal de improcedencia en los términos de la presente Ley.*

***Artículo 127.*** *En los casos en que a través del recurso de inconformidad se modifique o revoque la resolución del organismo garante, éste deberá emitir un nuevo fallo atendiendo los lineamientos que se fijaron al resolver la inconformidad, dentro del plazo de quince días, contados a partir del día siguiente al que se hubiere notificado o se tenga conocimiento de la resolución dictada en la inconformidad.*

***Artículo 128.*** *Corresponderá a los Organismos garantes, en el ámbito de su competencia, realizar el seguimiento y vigilancia del debido cumplimiento por parte del responsable de la nueva resolución emitida como consecuencia de la inconformidad en términos de la presente Ley.*

***Artículo 129.*** *Las resoluciones del Instituto serán vinculantes, definitivas e inatacables para los responsables y los Organismos garantes.*

*Los titulares podrán impugnar dichas resoluciones ante el Poder Judicial de la Federación mediante el Juicio de Amparo.*

## COMENTARIO

**Alessandra Barzizza y Mauricio Castillo**

### I. Antecedentes

Desde su creación, el INAI cuenta con facultades cuasi jurisdiccionales. Una de sus cuatro funciones principales es resolver aquellas controversias que se susciten entre la administración y los gobernados mediante un procedimiento seguido en forma de juicio.[258] La LFTAIPG (que precede a la LFTAIP) establecía que los particulares contaban con la posibilidad de interponer un recurso de revisión ante el IFAI en caso de que una unidad administrativa obligada les negara una solicitud de acceso a la información, declarase la inexistencia de documentos solicitados o se negase a efectuar entregas de datos personales o corregirlos, etc.

### II. Relevancia temática y contexto

Sin embargo, fue hasta enero de 2017, mediante la publicación de esta ley general, que se materializó la posibilidad de impugnar, ante el INAI, las resoluciones derivadas de un recurso de revisión emitidas por los organismos garantes de las entidades federativas en materia de protección de datos personales mediante el llamado recurso de inconformidad.

Lo anterior cobra sentido considerando el alcance de la reforma de 2014 al artículo 6º de la CPEUM, a través de la cual, el INAI se constituye en órgano garante del derecho a la protección de datos personales a nivel nacional. De tal forma que a través del recurso de inconformidad desarrollado en esta ley general se establece el procedimiento para que el Instituto actúe como órgano revisor de las resoluciones emitidas por los organismos garantes de las entidades federativas de los recursos de revisión que les competen. Todo lo cual resulta consecuente con el objetivo de la citada reforma constitucional para generar condiciones homogéneas que permitan generar estándares comunes de protección hacia las personas en toda la República Mexicana.

[258] Cfr. López Ayllón, S. (2005) "La creación de la Ley de Acceso a la Información en México: Una perspectiva desde el Ejecutivo federal", en Concha, H., López Ayllón, S. y Tacher, L. (Coords.), *Transparentar el Estado: La experiencia mexicana de acceso a la información*. México: Instituto de Investigaciones Jurídicas de la UNAM, p. 31.

## III. Análisis del contenido

De conformidad con el artículo 117 de la LGPDPPSO, el recurso de inconformidad puede interponerse por el titular de los datos personales o su representante ante el mismo organismo garante que emitió la resolución del recurso de revisión, o bien, de manera directa ante el INAI (dentro del plazo de quince días contados a partir del siguiente a la fecha de la notificación de la resolución impugnada). En el primer supuesto, el organismo garante que corresponda deberá remitirlo al INAI al día siguiente de haberlo recibido,[259] ya que este último es quien tiene la facultad exclusiva para conocer y resolver el recurso de inconformidad.

**1. Causales de procedencia.** Por su parte, el artículo 118, establece de manera taxativa las causales de procedencia del recurso de inconformidad: (1) porque la clasificación de los datos personales no cumpla con los requisitos de ley, (2) se determine la inexistencia de los datos personales o (3) se declare la negativa de los datos personales. En este último supuesto el legislador optó por una interpretación extensiva que incluye los datos personales incompletos o que no corresponden a lo solicitado; la negativa a los derechos ARCO; la utilización de formatos incomprensibles; costos de reproducción, envío o tiempos de entrega ante los que se inconforme el titular de los datos o su representante o porque se oriente a un trámite o procedimiento específico para solicitar el ejercicio de los derechos ARCO en contravención con lo dispuesto por el propio artículo 54 de esta ley.

**2. Requisitos del escrito de interposición del recurso.** El artículo 119 establece, de igual forma, los requisitos indispensables que deberá cumplir el escrito para interponer el recurso de inconformidad. Cabe destacar que dichos requisitos son únicos, lo cual implica que ni el INAI ni, en su caso, los organismos garantes de las entidades federativas, podrán exigir otros requisitos que los establecidos por la propia ley.

De hecho, los Lineamientos Generales de Protección de Datos Personales para el Sector Público precisan que “en ningún caso, será necesario que el titular [o su representante] ratifique el recurso de inconformidad”.[260] En caso de que alguno de estos requisitos no se cumpliera en el escrito de interposición del recurso de inconformidad, podría resultar procedente (1) la suplencia de

[259] “Artículo 167. En términos de lo dispuesto por el artículo 117 de la Ley General, cuando el titular o su representante presenten el recurso de inconformidad ante el organismo garante que emitió la resolución, éste de considerarlo necesario, podrá remitir junto con el recurso de inconformidad un informe justificado para acreditar la legalidad de su resolución previsto en el Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público”, *Diario Oficial de la Federación,* 26 de enero de 2018.

[260] Cfr. Artículo 168 del Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público, *Diario Oficial de la Federación,*26 de enero de 2018.

la queja por parte del Instituto o (2) si ésta no fuera posible, un acuerdo de prevención al titular, por una sola ocasión, para que subsane las omisiones respectivas. En caso de que dichas omisiones no sean subsanadas dentro del plazo de quince días a partir de la notificación, el recurso de inconformidad será desechado, de conformidad con lo dispuesto por el artículo 122 de la LGPDPPSO. Cabe advertir que la prevención tiene por efecto suspender el plazo para resolver el recurso de inconformidad.

**3. La suplencia de la queja.** El artículo 121 de la LGPDPPSO establece que, en el recurso de inconformidad, el INAI deberá suplir la deficiencia de la queja a favor del titular. Lo anterior bajo la condición de que no altere el contenido original del recurso de inconformidad, ni modifique los hechos o peticiones expuestas en el mismo. Asimismo, el INAI debe garantizar que las partes puedan presentar los argumentos y constancias que funden y motiven sus pretensiones.

La suplencia de la queja es una institución procesal que opera siempre a favor de la parte quejosa.[261] Su objeto es evitar que las deficiencias de carácter técnico-jurídico sean un impedimento para el acceso efectivo a la justicia, o bien, provoquen una situación de desigualdad para alguna de las partes en el proceso.[262] Si bien en el recurso de inconformidad no opera propiamente la figura del quejoso, ya que dicho concepto corresponde al juicio de amparo, en este caso la parte susceptible de sufrir una vulneración es el titular. En virtud de lo anterior, la suplencia de la queja operaría siempre a favor del titular en caso de que decida impugnar la resolución del organismo garante emitido en el recurso de revisión respectivo.

El alcance del ejercicio de la facultad de suplir la deficiencia de la queja es un tema controversial en la práctica. Por un lado, el principio de estricto derecho requiere que el juzgador examine los agravios o conceptos de violación de las demandas o recursos tal como fueron planteados por las partes. En ese mismo sentido, el principio de imparcialidad obliga a las autoridades jurisdiccionales a dirigir y resolver el juicio sin favorecer indebidamente a ninguna de las partes.[263]

---

[261] SUPLENCIA DE LA QUEJA. NO PROCEDE RESPECTO DE LAS AUTORIDADES RESPONSABLES. Suprema Corte de Justicia de la Nación. Tesis aislada, Séptima Época, *Semanario Judicial de la Federación y su Gaceta*, marzo de 1982, vol. 157-162, Primera Parte, p. 232.

[262] SUPLENCIA DE LA QUEJA DEFICIENTE EN EL JUICIO DE AMPARO. DEBE ANALIZARSE ACORDE CON EL MARCO SOBRE DERECHOS HUMANOS RESGUARDADO POR EL ARTÍCULO 1º DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, A PARTIR DE LA REFORMA PUBLICADA EN EL DIARIO OFICIAL DE LA FEDERACIÓN EL 10 DE JUNIO DE 2011. Suprema Corte de Justicia de la Nación. Tesis jurisprudencial 2a./J. 154/2015, Décima Época, *Semanario Judicial de la Federación y su Gaceta*, Libro 25, diciembre de 2015, Tomo I, p. 317.

[263] IMPARCIALIDAD. CONTENIDO DEL PRINCIPIO PREVISTO EN EL ARTÍCULO 17 CONSTITUCIONAL. Suprema Corte de Justicia de la Nación. Tesis jurisprudencial 1a./J. 1/2012, Novena Época, *Semanario Judicial de la Federación y su Gaceta*, Libro V, octubre de 2005, Tomo I, p. 460.

Por otro lado, la suplencia de la queja obliga al juzgador a suplir las deficiencias que encuentre en el planteamiento de la demanda o recurso, siempre a favor de la parte agraviada.[264]

Aunque existen criterios jurisprudenciales en los que se aborda el problema anteriormente planteado, éstos no han sido consistentes. En algunos criterios se ha establecido que la facultad de suplir la deficiencia de la queja no es ilimitada, sino que debe realizarse a partir de lo expresado en los conceptos de violación o agravios, a excepción de la materia penal.[265] Sin embargo, en otros criterios más recientes, basados en la nueva Ley de Amparo, se establece que el juzgador debe discernir caso por caso — y dependiendo de la materia y sujeto del que se trate — si es que existen violaciones manifiestas no resueltas en el procedimiento de origen que afecten al quejoso o recurrente. Lo anterior, aun ante la ausencia de conceptos de violación o agravios relacionados con la violación e independientemente de la materia de que se trate.[266]

Respecto al alcance del ejercicio de esta facultad por parte del INAI, esta ley general establece que debe ser ejercida únicamente bajo la condición de que no modifique el contenido original del recurso ni los hechos o peticiones expuestas en el mismo. De una interpretación literal de este artículo se desprende que esta facultad debe ejercerse, únicamente, a partir de lo expresado en los agravios del recurso. Sin embargo, creemos que, a pesar de lo que se establece en dicho precepto, el principio pro persona obliga al INAI a adoptar el criterio de interpretación más amplio respecto al alcance del ejercicio de esta facultad. Es decir, el INAI deberá discernir, caso por caso, y dependiendo de la materia y sujeto del que se trate (bajo criterios de necesidad y razonabilidad), si es que existen violaciones manifiestas no resueltas en el procedimiento de origen que afecten al titular.

**4. Pruebas y alegatos.** Una vez admitido el recurso de inconformidad, el expediente se pone a disposición de las partes para que en el plazo de siete días (a partir de la notificación del acuerdo de admisión del recurso) manifiesten lo que a su derecho convenga y ofrezcan las pruebas que consideren pertinentes, mismas que podrán ser admitidas o desechadas de acuerdo con

[264] Pérez, A. (2017). "Los principios del Juicio de Amparo" en Pérez Daza, Alfonso (Coord.), *El principio de estricto derecho en el juicio de amparo. Alcance y consecuencias del mismo conforme a la legislación, la doctrina y la jurisprudencia*. México: Consejo de la Judicatura, p. 22-24.

[265] SUPLENCIA DE LA QUEJA DEFICIENTE. DEBE HACERSE A PARTIR DE LOS CONCEPTOS DE VIOLACIÓN O, EN SU CASO, DE LOS AGRAVIOS EXPRESADOS, POR LO TANTO NO ES ILIMITADA. Suprema Corte de Justicia de la Nación. Tesis jurisprudencial 1a./J. 35/2005, Novena Época, *Semanario Judicial de la Federación y su Gaceta*, abril de 2005, Tomo XXI, p. 686.

[266] SUPLENCIA DE LA QUEJA DEFICIENTE. SU PROCEDENCIA EN OTRAS MATERIAS, AUN A FALTA DE CONCEPTO DE VIOLACIÓN O AGRAVIO, CUANDO SE ADVIERTA VIOLACIÓN GRAVE Y MANIFIESTA DE LA LEY. Suprema Corte de Justicia de la Nación. Tesis 2a./J. 120/2015, Décima Época, *Semanario Judicial de la Federación y su Gaceta*, Libro 22, septiembre de 2015, Tomo I, p. 663.

esta ley y los Lineamientos Generales de Protección de Datos Personales para el Sector Público.[267] Una vez concluida la etapa del desahogo de pruebas, se pone a disposición de las partes (y en su caso terceros interesados), mediante un acuerdo, todas las actuaciones realizadas, a fin de que formulen alegatos dentro del plazo de cinco días contados a partir de dicho acuerdo.

**5. Resolución.** De conformidad con el artículo 124 de la LGPDPPSO, la resolución del INAI de los recursos de inconformidad podrá sobreseer o desechar el recurso, confirmar, revocar o modificar la resolución del organismo garante, o bien, ordenar la entrega de los datos personales, en caso de omisión del responsable.

Si bien la LGPDPPSO establece en su artículo 120 que el INAI cuenta con el plazo de 30 días, prorrogables en una sola ocasión por un período igual, contado a partir del día siguiente a la interposición del recurso de inconformidad, sin distinguir si el recurso de inconformidad fue interpuesto de manera directa ante el Instituto o si se realizó a través del organismo garante de la entidad federativa, los Lineamientos Generales de Protección de Datos Personales para el Sector Público especifican que en caso de que el recurso haya sido interpuesto ante dichos organismos garantes, los 30 días empezarán a correr a partir de la recepción del recurso de inconformidad en el Instituto.[268]

**6. Negativa ficta.** El artículo 124 de esta ley general establece que, en caso de que el INAI no resuelva el recurso de inconformidad dentro de los plazos establecidos en el artículo 120, la resolución emitida por el organismo garante —aquella que fue objeto del recurso de inconformidad— se entenderá confirmada. A esta figura jurídica se le conoce como negativa ficta y tiene por objeto brindar seguridad jurídica a los particulares mediante la sustitución del acto expreso por parte de la autoridad. De esta manera se activan los medios de defensa que normalmente procederían en contra de las resoluciones expresas emitidas por dicha autoridad.[269]

La interpretación jurisprudencial respecto a la naturaleza jurídica de las respuestas fictas no ha sido consistente y presenta diversas problemáticas. Por un lado, se ha considerado que las respuestas fictas son un hecho jurídico, por lo que no son impugnables por falta de fundamentación y motivación ni deben ser interpretadas, ya que la voluntad de la autoridad no interviene en la actualización

[267] Cfr. Artículos 173 y 174 del Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público, *Diario Oficial de la Federación,* 26 de enero de 2018.

[268] Cfr. Artículo 178 del Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público, *Diario Oficial de la Federación,* 26 de enero de 2018.

[269] Roldán, J. (2008). "El silencio de la administración", en *Derecho Administrativo*. México: Oxford University Press, p. 328-340.

de la hipótesis normativa que las contiene.[270] Por otro lado, se les considera un acto jurídico, por lo que pueden ser impugnadas por falta de fundamentación y motivación. Estos elementos serán brindados por la autoridad en un momento procesal posterior.[271] Por último, en un criterio más reciente, se estableció que las respuestas fictas "no constituyen un verdadero acto, sino son una ficción legal de efectos exclusivamente procesales que opera en beneficio del particular, superando los efectos del silencio de la administración".[272]

Como puede apreciarse de lo anteriormente planteado, la discusión respecto de la naturaleza jurídica de las respuestas fictas no está agotada. Sin embargo, es posible afirmar que dicha figura, sin duda, brinda seguridad jurídica a los titulares, pues una de las consecuencias que se derivan de su actualización es, precisamente, la activación de medios de impugnación. Por ejemplo, en el caso de esta ley general, la actualización de la hipótesis normativa contenida en el artículo 124 trae como consecuencia necesaria la activación del derecho del titular de recurrir al amparo. *Mutatis mutandis*, la negativa ficta contemplada en esta ley general brinda al titular la posibilidad de combatir, por medio del amparo, una resolución negativa por parte del organismo garante en caso de falta de respuesta por parte del INAI.

**7. La responsabilidad de los servidores públicos.** El artículo 124 de la LGPDPPSO establece que, durante la sustanciación del recurso de inconformidad, el INAI se encuentra facultado para denunciar el posible incumplimiento por parte de servidores públicos con las obligaciones establecidas en esta ley general o cualquier otra disposición aplicable a la materia. Lo anterior con la finalidad de que el órgano interno de control o la instancia competente para hacerlo inicien el procedimiento de responsabilidad que corresponda.

De conformidad con lo establecido en diversos preceptos constitucionales, la responsabilidad de los servidores públicos tiene distintas vertientes: penal, civil, política, resarcitoria y administrativa. Existen órganos competentes y procedimientos distintos para la imputación de cada uno de los tipos de responsabilidad que se describen. La activación de uno de estos procedimientos no excluye la posibilidad de recurrir a otros.[273]

---

[270] NEGATIVA FICTA. NO PUEDE IMPUGNARSE POR FALTA DE FUNDAMENTACIÓN Y MOTIVACIÓN. Segundo Tribunal Colegiado en Materia Administrativa del Primer Circuito. Tesis aislada, Octava Época, *Semanario Judicial de la Federación y su Gaceta,* junio de 1991, Tomo VII, p. 331.

[271] NEGATIVA FICTA, NO PROCEDE SU IMPUGNACIÓN ANTE LA PROPIA AUTORIDAD QUE INCURRIÓ EN LA. Cuarto Tribunal Colegiado en Materia Administrativa del Primer Circuito. Tesis aislada, Octava Época, *Semanario Judicial de la Federación y su Gaceta*, septiembre de 1991, Tomo VIII, p. 161.

[272] NEGATIVA FICTA REGULADA EN EL CÓDIGO FISCAL DE LA FEDERACIÓN. NO PUEDE SER RECLAMADA MEDIANTE EL JUICIO DE AMPARO INDIRECTO, EN ATENCIÓN A SU NATURALEZA Y AL PRINCIPIO DE DEFINITIVIDAD. Cuarto Tribunal Colegiado en Materia Administrativa del Primer Circuito, Tesis, Octava Época, *Semanario Judicial de la Federación y su Gaceta*, Tomo VIII, septiembre de 1991, p. 161.

[273] Cfr. López, M. (2013). "El sistema federal de responsabilidades de los servidores públicos" y

La prevención, detección y sanción de responsabilidades administrativas de los servidores públicos es una materia concurrente entre la Federación y los estados. La Ley General de Responsabilidades Administrativas (LGRA), cuyo objeto es la distribución de competencias en esta materia, establece que la Secretaría de la Función Pública, sus equivalentes en las entidades federativas, los órganos internos de control, la Auditoría Superior de la Federación y las autoridades de fiscalización superior de las entidades federativas son competentes para investigar y posteriormente calificar las faltas administrativas como graves o no graves. Este proceso de calificación es importante, ya que de su resultado depende quién será la autoridad encargada de dirigir, continuar y resolver el procedimiento de responsabilidad administrativa.

En caso de que una falta administrativa sea calificada como no grave, la resolución del procedimiento de responsabilidad administrativa corresponderá al órgano interno de control o la unidad de responsabilidades administrativas de la dependencia o entidad que sea señalada como presunto responsable. En cambio, cuando la falta sea calificada como grave, el resto del procedimiento será dirigido por la Secretaría de la Función Pública o sus homólogas en las entidades federativas, los órganos internos de control, la Auditoría Superior de la Federación o sus equivalentes, según corresponda, y posteriormente resuelto por el Tribunal de Justicia Administrativa competente. Aunque la calificación de las faltas administrativas como graves o no graves corresponde a la autoridad investigadora, éstas ya se encuentran clasificadas en la LGRA y existen medios de impugnación que puede activar la parte denunciante en caso de desacuerdo con la calificación que se les otorgue.

La autonomía que guardan los órganos internos de control es un factor que sin duda opera a favor del cumplimiento de los principios rectores del servicio público establecidos en el título cuarto de la Constitución y, por lo tanto, del cumplimiento por parte de los servidores públicos con sus obligaciones. Los titulares de los órganos internos de control no dependen funcional ni jerárquicamente de los entes públicos a los que pertenecen, y la facultad de designar a los titulares de los órganos internos de control, en el caso de las entidades de la administración pública federal, pertenece a la Secretaría de la Función Pública y a la Cámara de Diputados en el caso de los órganos constitucionales autónomos.

En virtud de lo anterior, consideramos que la facultad que esta ley general otorga al INAI para denunciar una probable responsabilidad administrativa reafirma su posicionamiento como órgano garante nacional. Sin embargo, la eficacia de este mecanismo no dependerá del INAI, sino del correcto

"Sobre los principios que rigen la actuación de los servidores públicos", en *La responsabilidad administrativa de los servidores públicos en México*. México: Instituto de Investigaciones Jurídicas de la UNAM, p. 37 y 98.

funcionamiento y cabal cumplimiento por parte de las entidades encargadas de investigar y sancionar las faltas administrativas que se denuncien.

**8. Procedencia del amparo.** El amparo es una institución procesal cuya finalidad es proteger los derechos humanos establecidos en la Constitución y en los tratados internacionales de los que México sea parte. Este medio de defensa puede tramitarse vía directa o indirecta y procede en contra de normas generales, actos u omisiones de autoridades o particulares (en algunos supuestos) que violen los derechos anteriormente mencionados. El artículo 129 de esta ley general establece que los titulares pueden impugnar las resoluciones del INAI mediante juicio de amparo, sin embargo, no establece expresamente cuál es la vía —directa o indirecta— que resulta procedente en contra de dichas resoluciones.

El amparo directo procede en contra de sentencias definitivas, laudos o resoluciones que pongan fin a juicio dictadas por tribunales judiciales, administrativos o de trabajo. Considerando que el INAI no es un órgano de naturaleza jurisdiccional, sus resoluciones no son objeto de amparo directo. En virtud de lo anterior, creemos que la vía idónea para ampararse en contra de las resoluciones del INAI es la indirecta. Lo anterior encuentra sustento en el artículo 107, fracciones II y III de la Ley de Amparo. La fracción II establece que el amparo indirecto procede contra actos u omisiones que provengan de autoridades distintas a los tribunales judiciales, administrativos o del trabajo. La fracción III establece que procede contra resoluciones provenientes de un procedimiento administrativo seguido en forma de juicio (siempre que se actualice alguno de los supuestos establecidos en los incisos de dicha fracción).

Recordemos que la procedencia del amparo que, en su caso, interponga el titular también se encuentra condicionada por el principio de definitividad en el juicio de amparo. Este principio consiste en agotar el recurso, juicio o medio ordinario de defensa legal por virtud del cual pudiere modificarse el acto u omisión materia del amparo. En virtud de que el recurso de inconformidad es la última instancia que, de acuerdo con esta ley general, el titular puede agotar para impugnar las resoluciones emitidas por el organismo garante, creemos que una vez agotado este recurso, el amparo resulta procedente.

## IV. Conclusiones

El recurso de inconformidad previsto en la LGPDPPSO constituye una manifestación del carácter nacional del INAI, a través del otorgamiento de facultades que le permiten generar condiciones comunes para dotar de efectividad el derecho humano a la protección de datos personales en todo el país por medio de una instancia adicional para conocer las resoluciones de los organismos garantes de las entidades federativas en los recursos de revisión.

## Referencias

Cuarto Tribunal Colegiado en Materia Administrativa del Primer Circuito. (septiembre 1991). Tesis aislada, Octava Época, *Semanario Judicial de la Federación y su Gaceta*, Tomo VIII, p. 161.

DOF. (2018). Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público, *Diario Oficial de la Federación*.

López, M. (2013). “El sistema federal de responsabilidades de los servidores públicos” y “Sobre los principios que rigen la actuación de los servidores públicos”, en *La responsabilidad administrativa de los servidores públicos en México*. México: Instituto de Investigaciones Jurídicas de la UNAM.

López Ayllón, S. (2005). “La creación de la Ley de Acceso a la Información en México: Una perspectiva desde el Ejecutivo federal”, en Concha Cantú, Hugo, López Ayllón, Sergio y Tacher Epelstein, Lucy (Coords.), *Transparentar el Estado: La experiencia mexicana de acceso a la información.* México: Instituto de Investigaciones Jurídicas de la UNAM.

Pérez, A. (2017). “Los principios del Juicio de Amparo”, en Pérez Daza, Alfonso (Coord.), *El principio de estricto derecho en el juicio de amparo. Alcance y consecuencias del mismo conforme a la legislación, la doctrina y la jurisprudencia*. México: Consejo de la Judicatura.

Roldán, J. (2008). “El silencio de la administración”, en *Derecho Administrativo*. México: Oxford University Press.

Segundo Tribunal Colegiado en Materia Administrativa del Primer Circuito. (junio 1991). Tesis aislada, Octava Época, *Semanario Judicial de la Federación y su Gaceta*. Tomo VII, p. 331.

Suprema Corte de Justicia de la Nación. (marzo 1982). Tesis aislada, Séptima Época, *Semanario Judicial de la Federación y su Gaceta*, vol. 157-162, Primera Parte, p. 232.

Suprema Corte de Justicia de la Nación. (abril 2005). Tesis jurisprudencial 1a./J. 35/2005, Novena Época, *Semanario Judicial de la Federación y su Gaceta*. Tomo XXI, p. 686.

Suprema Corte de Justicia de la Nación. (octubre 2005). Tesis jurisprudencial 1a./J. 1/2012, Novena Época, *Semanario Judicial de la Federación y su Gaceta*, Libro V. Tomo I, p. 460.

Suprema Corte de Justicia de la Nación. (septiembre 2015). Tesis 2a./J. 120/2015, Décima Época, *Semanario Judicial de la Federación y su Gaceta*, Libro 22. Tomo I, p. 663.

Suprema Corte de Justicia de la Nación. (diciembre 2015). Tesis jurisprudencial 2a./J. 154/2015, Décima Época, *Semanario Judicial de la Federación y su Gaceta*, Libro 25. Tomo I, p. 317.

# CAPÍTULO IV
# DE LA ATRACCIÓN DE LOS RECURSOS DE REVISIÓN

***Artículo 130.*** *Para efectos de la presente Ley, el Pleno del Instituto, cuando así lo apruebe la mayoría de sus Comisionados, de oficio o a petición fundada de los Organismos garantes, podrá ejercer la facultad de atracción para conocer de aquellos recursos de revisión pendientes de resolución en materia de protección de datos personales, que por su interés y trascendencia así lo ameriten y cuya competencia original corresponde a los Organismos garantes, conforme a lo dispuesto en esta Ley y demás normativa aplicable.*

*Los recurrentes podrán hacer del conocimiento del Instituto la existencia de recursos de revisión que de oficio podría conocer.*

*Por lo que hace a los lineamientos y criterios generales de observancia obligatoria que el Instituto deberá emitir para determinar los recursos de revisión de interés y trascendencia que está obligado a conocer, conforme a la Ley General de Transparencia y Acceso a la Información Pública, adicionalmente en la atracción de recursos de revisión en materia de protección de datos personales se deberán considerar los siguientes factores:*

*I. La finalidad del tratamiento de los datos personales;*

*II. El número y tipo de titulares involucrados en el tratamiento de datos personales llevado a cabo por el responsable;*

*III. La sensibilidad de los datos personales tratados;*

*IV. Las posibles consecuencias que se derivarían de un tratamiento indebido o indiscriminado de datos personales, y*

*V. La relevancia del tratamiento de datos personales, en atención al impacto social o económico del mismo y del interés público para conocer del recurso de revisión atraído.*

***Artículo 131.*** *Para efectos del ejercicio de la facultad de atracción a que se refiere este Capítulo, el Instituto motivará y fundamentará que el caso es de tal relevancia, novedad o complejidad, que su resolución podrá repercutir de manera sustancial en la solución de casos futuros para garantizar la tutela efectiva del derecho de protección de datos personales en posesión de sujetos obligados.*

*En los casos en los que el organismo garante de la Entidad Federativa sea el sujeto obligado recurrido, deberá notificar al Instituto, en un plazo que no excederá de tres días, a partir de que sea interpuesto el recurso. El Instituto atraerá y resolverá dichos recursos de revisión, conforme a lo establecido en el presente Capítulo.*

***Artículo 132.*** *Las razones emitidas por el Instituto para ejercer la facultad de atracción de un caso, únicamente constituirán un estudio preliminar para determinar si el asunto reúne los requisitos constitucionales y legales de interés y trascendencia, conforme al precepto anterior, por lo que no será necesario que formen parte del análisis de fondo del asunto.*

***Artículo 133.*** *El Instituto emitirá lineamientos y criterios generales de observancia obligatoria que permitan determinar los recursos de revisión de interés y trascendencia que estará obligado a conocer, así como los procedimientos internos para su tramitación, atendiendo a los plazos máximos señalados para el recurso de revisión.*

***Artículo 134.*** *La facultad de atracción conferida al Instituto se deberá ejercer conforme a las siguientes reglas:*

*I. Cuando se efectúe de oficio, el Pleno del Instituto, cuando así lo aprueben la mayoría de sus Comisionados, podrá ejercer la atracción en cualquier momento, en tanto no haya sido resuelto el recurso de revisión por el organismo garante competente, para lo cual notificará a las partes y requerirá el Expediente al organismo garante correspondiente, o*

*II. Cuando la petición de atracción sea formulada por el organismo garante de la Entidad Federativa, éste contará con un plazo no mayor a cinco días, salvo lo dispuesto en el último párrafo del artículo 105 de esta Ley, para solicitar al Instituto que analice y, en su caso, ejerza la facultad de atracción sobre el asunto puesto a su consideración.*

*Transcurrido dicho plazo se tendrá por precluido el derecho del organismo garante respectivo para hacer la solicitud de atracción.*

*El Instituto contará con un plazo no mayor a diez días para determinar si ejerce la facultad de atracción, en cuyo caso, notificará a las partes y solicitará el Expediente del recurso de revisión respectivo.*

***Artículo 135.*** *La solicitud de atracción del recurso de revisión interrumpirá el plazo que tienen los Organismos garantes para resolverlo. El cómputo continuará a partir del día siguiente al día en que el Instituto haya notificado la determinación de no atraer el recurso de revisión.*

***Artículo 136.*** *Previo a la decisión del Instituto sobre el ejercicio de la facultad de atracción a que se refiere el artículo anterior, el organismo garante de la Entidad Federativa a quien corresponda el conocimiento originario del asunto, deberá agotar el análisis de todos los aspectos cuyo estudio sea previo al fondo del asunto, hecha excepción del caso en que los aspectos de importancia y trascendencia deriven de la procedencia del recurso.*

*Si el Pleno del Instituto, cuando así lo apruebe la mayoría de sus Comisionados, decide ejercer la facultad de atracción se avocará al conocimiento o estudio de fondo del asunto materia del recurso de revisión atraído.*

*El o los Comisionados que en su momento hubiesen votado en contra de ejercer la facultad de atracción, no estarán impedidos para pronunciarse respecto del fondo del asunto.*

***Artículo 137.*** *La resolución del Instituto será definitiva e inatacable para el organismo garante y para el sujeto obligado de que se trate.*

*En todo momento, los particulares podrán impugnar las resoluciones del Instituto ante el Poder Judicial de la Federación.*

***Artículo 138.*** *Únicamente el Consejero Jurídico del Gobierno podrá interponer recurso de revisión en materia de seguridad nacional ante la Suprema Corte de Justicia de la Nación, en el caso que las resoluciones del Instituto a los recursos descritos en este Título, puedan poner en peligro la seguridad nacional.*

*Dicho recurso de revisión en materia de seguridad nacional se tramitará en los términos que se establecen en el siguiente Capítulo V denominado "Del Recurso de Revisión en materia de Seguridad Nacional", del presente Título.*

## COMENTARIO

**María Solange Maqueo**

### I. Antecedentes

La facultad de atracción se introdujo en nuestro sistema jurídico en el año de 1987 mediante una reforma al artículo 107 de la CPEUM con el fin de constituir un medio de control de la legalidad conferido a la Suprema Corte de Justicia de la Nación y para conocer aquellos asuntos que, en materia de amparo, revistieran

"características especiales" (término que sería sustituido en 1994 por el de "interés" y "trascendencia"), pero que no correspondieran a su competencia originaria.[274] Posteriormente, esta facultad, prevista necesariamente en el orden constitucional, se hizo extensible a otros organismos gubernamentales, tales como la Comisión Nacional de Derechos Humanos, el Tribunal Electoral del Poder Judicial de la Federación, el Instituto Nacional Electoral y, de manera más reciente, a raíz de la reforma constitucional de 2014, el INAI.

## II. Relevancia temática y contexto

Si bien la facultad de atracción conferida a la Corte se explica como un mecanismo que permitiría mantener cierto poder de control de la legalidad al máximo tribunal del país en el marco de un proceso descentralizador del juicio de amparo, en el caso del INAI, la explicación obedece a un proceso inverso. La reforma constitucional de 2014 introdujo mecanismos que permitieron un mayor control centralizado en las materias de transparencia, acceso a la información pública y protección de datos personales en ámbitos que antes eran del exclusivo conocimiento de los órganos garantes de las entidades federativas. En ese contexto se sitúa la facultad de atracción del INAI, conjuntamente con el llamado recurso de inconformidad a que se refiere el Capítulo III del Título Noveno de esta ley general, mismos que dotan al INAI de una influencia de carácter "nacional". Ello, bajo el entendido de que estas medidas previstas por el orden constitucional permiten alcanzar uno de los objetivos propuestos por la propia reforma constitucional de 2014, en el sentido de generar estándares comunes de protección de datos personales en todo el territorio de la República Mexicana.

Así, la facultad de atracción del INAI se estableció a partir de la reforma constitucional al artículo 6º —específicamente, al apartado A, fracción VIII, párrafo quinto—, con la cual se faculta al INAI para conocer "de oficio o a petición fundada del organismo garante equivalente de las entidades federativas, […] de los recursos de revisión que por su interés y trascendencia así lo ameriten". De tal forma que, si bien a los órganos garantes de cada entidad federativa les corresponde originariamente conocer de los recursos de revisión que se planteen respecto de los sujetos obligados que se encuentren bajo su jurisdicción, el INAI, en el ejercicio de una facultad discrecional con rango constitucional, podrá atraer aquellos casos que, a su juicio, revistan interés y transcendencia. Se trata, pues, de una medida de carácter excepcional, cuyo ejercicio debe estar fundado y motivado en los criterios de interés y trascendencia, a fin de no hacer nugatorias las potestades de los órganos garantes estatales para conocer de los recursos de revisión que le corresponden.

[274] Cfr. Suárez, A. (2017). "Usos e interpretación de la facultad de atracción en el juicio de amparo por la SCJN", en Ferrer Mac-Gregor, Eduardo y Herrera, Alonso (Coords.), *El juicio de amparo en el centenario de la Constitución mexicana de 1917. Pasado, Presente y Futuro*, Tomo I. México: Instituto de Investigaciones Jurídicas de la UNAM, p. 464.

## III. Análisis del contenido

**1. Requisitos de interés y trascendencia.** El presente Capítulo IV de la LGPDPPSO desarrolla el procedimiento y los criterios de interés y trascendencia para el ejercicio de la facultad de atracción de los recursos de revisión prevista por el orden constitucional "en materia de protección de datos personales". No obstante, la propia ley general pretende adoptar mecanismos compatibles y estandarizados con el ejercicio de la facultad de atracción del INAI en materia de transparencia y acceso a la información pública. De hecho, como se observa en el artículo 130 de esta ley, existe una remisión expresa a los lineamientos y criterios generales que se emitan de conformidad con la LGTAIP, de tal forma que, a través de esta remisión, se habilita la posibilidad de regular de manera unificada el ejercicio de la facultad de atracción de los recursos de revisión independientemente de la materia de origen.

Sin embargo, en términos del propio artículo 130 de la LGPDPPSO, el análisis para determinar la procedencia de la facultad de atracción de los recursos de revisión en materia de protección de datos personales, debe considerar algunas situaciones específicas propias de este derecho, por ejemplo: (1) la finalidad del tratamiento de los datos personales, (2) el número y tipo de titulares involucrados en su tratamiento (3), el carácter sensible de los datos personales, (4) las consecuencias que podrían derivarse de un tratamiento indebido o indiscriminado y (5) la relevancia del tratamiento de los datos personales en atención al impacto social o económico del mismo y del interés público para conocer del recurso de revisión atraído. Estos criterios de análisis deberán ser considerados al momento de regular la facultad de atracción en esta materia,[275] así como para valorar y motivar, en cada caso, la procedencia de esta facultad en atención a las características de interés o trascendencia que justifiquen la atracción de los recursos de revisión.

En relación con lo anterior, el artículo 131 de esta ley general establece algunas pautas que permiten dotar de significado a los criterios de interés y trascendencia. En principio se trata de casos "de tal relevancia, novedad o complejidad, que su resolución [pueda]… repercutir de manera sustancial en la solución de casos futuros para garantizar la tutela efectiva del derecho de protección de datos personales en posesión de sujetos obligados".

Estas pautas no sólo son plenamente coincidentes con lo dispuesto por el artículo 182 de la LGTAIP, sino que además, resultan compatibles con el

[275] Cfr. Artículo 6 in fine del "Acuerdo mediante el cual se aprueba reformar los artículos 2, fracciones II, III, V, VI, IX, X, XII, XIII, XIV, XV y XVI; 4; 6; 9, fracciones II, incisos A y B, y XII; 11, fracción III; 12, apartado A, fracción III, y apartado C, fracción II, y 13 de los Lineamientos Generales para que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ejerza la facultad de atracción", *Diario Oficial de la Federación,* 26 de enero de 2018.

desarrollo jurisprudencial de la Suprema Corte de Justicia de la Nación respecto de la facultad de atracción. En ese sentido, la Corte ha sostenido que el interés y la trascendencia, "como requisitos que justifican el ejercicio de la facultad de atracción", si bien referida a sus propias facultades aunque extrapolables para el caso del INAI, "se orientan a calificar un asunto que por los problemas jurídicos planteados, dada su relevancia, novedad o complejidad, requieren de un pronunciamiento del máximo tribunal del país, de tal suerte que el criterio que llegara a sustentarse repercutirá de manera excepcionalmente importante en la solución de casos futuros".[276]

De igual forma, la Corte ha precisado que los criterios de interés y trascendencia comprenden elementos tanto de carácter cualitativo como cuantitativo. En ese sentido, señala que "[…] se estima necesario utilizar los conceptos 'interés' e 'importancia' como notas relativas a la naturaleza intrínseca del caso, tanto jurídica como extrajurídicamente, para referirse al aspecto cualitativo, y reservar el concepto de 'trascendencia' para el aspecto cuantitativo, para así reflejar el carácter excepcional o novedoso que entrará la fijación de un criterio estrictamente jurídico. Además, la trascendencia se deriva de la complejidad sistémica que presentan algunos asuntos por su interdependencia jurídica o procesal; esto es, aquellos que están relacionados entre sí de tal forma que se torna necesaria una solución que atienda a las consecuencias jurídicas de todos y cada uno de ellos".

La Corte sostiene que el ejercicio de la facultad de atracción implica el cumplimiento conjunto de dos requisitos: 1) que la naturaleza intrínseca del caso permita advertir un interés superlativo reflejado en la gravedad del tema "es decir, en la posible afectación o alteración de los valores sociales, políticos o, en general, de convivencia, bienestar o estabilidad del Estado" y 2) que el caso revista trascendencia reflejada "en lo excepcional o novedoso que entrañaría la fijación de un criterio jurídico trascendente para casos futuros o la complejidad sistémica de los mismos".[277] Como se advierte de esta tesis jurisprudencial de la Suprema Corte, la facultad de atracción requiere entonces que se actualicen ambos criterios, esto es, tanto el interés como la trascendencia del caso, para su procedencia. Entonces, no se trata de justificar o motivar la existencia de un criterio u otro, sino la concurrencia de ambos.

Con influencia directa de estas ideas, el Acuerdo mediante el cual se aprueban los nuevos Lineamientos generales para que el INAI ejerza la

[276] FACULTAD DE ATRACCIÓN. EL INTERÉS Y TRASCENDENCIA QUE JUSTIFICAN SU EJERCICIO SON DE ÍNDOLE JURÍDICA. Suprema Corte de Justicia de la Nación. Tesis 2a./J. 143/2006, *Semanario Judicial de la Federación y su Gaceta*, Novena Época, octubre de 2006, Tomo XXIV, p. 335.

[277] FACULTAD DE ATRACCIÓN. REQUISITOS PARA SU EJERCICIO. Suprema Corte de Justicia de la Nación. Tesis jurisprudencial 1a./J. 27/2008, *Semanario Judicial de la Federación y su Gaceta*, Novena Época, abril de 2008, Tomo XXVII, p. 150.

facultad de atracción, emitido por el INAI y publicado en el DOF el 16 de febrero de 2017, establece, en su artículo 6, el sentido y alcance de los criterios de interés y trascendencia:

I. Interés: requisito de carácter cualitativo que denota el interés e importancia jurídica, histórica, política, económica, social, que se deriva de la naturaleza intrínseca del caso, debido a la gravedad, trascendencia, complejidad, importancia o impacto del tema en virtud de que la resolución de éste reviste gran relevancia reflejada en la gravedad del tema por ser fundamental para la protección del ejercicio del derecho de acceso a la información o protección de datos personales en posesión de sujetos obligados, y

II. Trascendencia: requisito cuantitativo que denota la excepcionalidad o carácter extraordinario del caso, por ser novedoso, no tener precedentes o similitud con alguno otro, de tal modo que su resolución entrañaría la fijación de un criterio normativo para casos futuros cuando la materia del recurso de revisión sea de tal excepción, novedad o complejidad que su resolución podría repercutir de manera sustancial en casos futuros para garantizar la tutela efectiva del derecho de acceso a la información y protección de datos personales en posesión de los sujetos obligados, o bien, que supondría la fijación de un criterio jurídico sobresaliente para casos futuros o la complejidad sistémica de los mismos.

Ahora bien, esta ley general, en su artículo 131, segundo párrafo establece un supuesto de excepción al carácter potestativo y discrecional del INAI para ejercer su facultad de atracción y en el que la calificación de los requisitos de interés y trascendencia escapan del ámbito de valoración del INAI para estar determinados de manera directa por la ley. Se trata de los recursos de revisión interpuestos ante los organismos garantes de las entidades federativas y en los que son ellos mismos los sujetos recurridos en su carácter de sujetos obligados o responsables del tratamiento de datos personales. Sin duda alguna, esta disposición y, con ello, el entendimiento de sus características de interés y trascendencia, van de la mano con la existencia de un posible conflicto de interés que justifica, de acuerdo con el propio legislador, la intervención del órgano garante de carácter nacional.

**2. Procedimientos.** De acuerdo con el artículo 130 de la LGPDPPSO, el INAI podrá conocer de los recursos de revisión que no corresponden a su competencia originaria, sea de oficio o a petición fundada de los órganos garantes de las entidades federativas.

Tratándose del ejercicio de esta facultad de manera oficiosa, la ley general establece que podrán ser los propios recurrentes quienes hagan del conocimiento

del INAI la existencia de recursos de revisión que podrían ser susceptibles de atracción, caso en el cual, no necesitarían acreditar el interés y trascendencia del asunto, dado que esta función correspondería precisamente al INAI.

De igual forma, los lineamientos generales para que el INAI ejerza la facultad de atracción de 2017 y modificados en enero de 2018 establecen otras vías a través de las cuales podrían identificarse aquellos recursos de revisión pendientes de resolución por parte de los órganos garantes de las entidades federativas que podrían revestir las características de interés y trascendencia. La primera, se refiere a un esquema de monitoreo o seguimiento por parte de la Secretaría Ejecutiva del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales de los recursos de revisión interpuestos ante los órganos garantes estatales y, la segunda, comprende la solicitud fundada y motivada que realice cualquiera de los comisionados que conforman el Pleno del INAI.[278] Sin duda esta segunda vía corresponde a una aplicación por analogía de criterios jurisprudenciales sostenidos por la Suprema Corte de Justicia de la Nación para sus propias facultades de atracción.[279] Cabe advertir que los Lineamientos para el ejercicio de la facultad de atracción de 2016, ahora abrogados, preveían también el supuesto de que el Consejo Consultivo del INAI pudiera hacer del conocimiento del Instituto este tipo de asuntos. No obstante, los nuevos Lineamientos de 2017 ya no contemplan este supuesto.

El ejercicio de la facultad de atracción de oficio puede realizarse en cualquier momento o etapa procesal en la que se encuentre el recurso de revisión interpuesto ante los órganos garantes de las entidades federativas, siempre y cuando aún no haya sido resuelto, para lo cual, en términos de la fracción I del artículo 134 de esta ley, el INAI notificará a las partes y requerirá el expediente al órgano garante que corresponda.

Ahora bien, por lo que se refiere al procedimiento para el ejercicio de la facultad de atracción a petición fundada de los órganos garantes estatales, la fracción II del artículo 134 de esta ley establece el plazo de cinco días (hábiles) para su formulación. En su solicitud, el órgano garante correspondiente, deberá argumentar por qué considera que el caso cumple con los requisitos de interés y trascendencia. En el supuesto excepcional de que la solicitud se presente por tratarse del órgano recurrido, el plazo para notificar al INAI es tan sólo de

[278] Cfr. Artículo 12 del "Acuerdo mediante el cual se aprueba reformar los artículos 2, fracciones II, III, V, VI, IX, X, XII, XIII, XIV, XV y XVI; 4; 6; 9, fracciones II, incisos A y B, y XII; 11, fracción III; 12, apartado A, fracción III, y apartado C, fracción II, y 13 de los Lineamientos Generales para que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ejerza la facultad de atracción", *Diario Oficial de la Federación,* 26 de enero de 2018.

[279] ATRACCIÓN, FACULTAD DE. SU EJERCICIO PUEDE SOLICITARSE OFICIOSAMENTE POR LOS MINISTROS DE LA SUPREMA CORTE DE JUSTICIA. Suprema Corte de Justicia de la Nación. Tesis P.CXLVIII/96, *Semanario Judicial de la Federación y su Gaceta*, Novena Época, diciembre de 1996, Tomo IV, p. 109.

tres días a partir de la interposición del recurso como lo prevé el artículo 131 *in fine* aunque no requiere de una justificación específica sobre su interés y trascendencia, pues su procedencia viene determinada por la propia ley.

En cualquiera de ambos supuestos, sea de oficio o a petición fundada de los organismos garantes de las entidades federativas, el Pleno del INAI tiene diez días para resolver sobre el ejercicio de la facultad de atracción, misma que podrá adoptarse por mayoría simple de los comisionados. Bajo este supuesto, el INAI deberá notificar a las partes y solicitar el expediente del recurso de revisión respectivo. En cualquier caso, previo a la resolución del INAI sobre el ejercicio de la facultad de atracción, el organismo garante que corresponda deberá haberse pronunciado sobre la admisión del recurso de revisión o sobre cualquier otra cuestión previa al análisis de fondo, a menos que dichas cuestiones sean precisamente las que hubieren motivado la posible atracción del recurso.

Finalmente, cabe decir que el proceso ante el INAI para determinar la procedencia de la facultad de atracción tiene por efecto "suspender" (más que interrumpir como con poca precisión jurídica establece el artículo 135 de la LGPDPPSO) el plazo con que cuentan los organismos garantes para la resolución de los recursos de revisión correspondientes. En el supuesto de que el INAI determinara que no procede la atracción del recurso de revisión, entonces, se reanudaría el cómputo del plazo a partir del día hábil siguiente a la notificación de esta decisión.

**3. Naturaleza de la facultad de atracción.** Si bien el análisis para determinar la procedencia del ejercicio de la facultad de atracción implica el examen del recurso de revisión en su integridad, pues sólo de esta forma podría verificarse el cumplimiento de los requisitos de interés y trascendencia, ello no supone en ningún caso prejuzgar sobre el fondo del asunto. De hecho, tal como se expresa en el artículo 132 de la LGPDPPSO, las razones emitidas por el INAI para ejercer la facultad de atracción constituyen "un estudio preliminar para determinar si el asunto reúne los requisitos constitucionales y legales de interés y trascendencia, […], por lo que no será necesario que formen parte del análisis del fondo del asunto." Esta disposición normativa encuentra sus antecedentes en los criterios jurisprudenciales de la Suprema Corte de Justicia de la Nación emitidos con base en el análisis de su propia facultad de atracción. Al respecto, este máximo tribunal ha sostenido que: "[l]as razones emitidas […] para ejercer la facultad de atracción en un caso no son de estudio obligado al analizarse el fondo del asunto, porque la naturaleza de dicha facultad es la de un estudio preliminar que tiene como fin determinar [si se reúnen]… los requisitos constitucionales de 'interés' y 'trascendencia', […]".[280]

[280] FACULTAD DE ATRACCIÓN. LAS RAZONES EMITIDAS POR LA PRIMERA SALA DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN PARA EJERCERLA NO SON DE ESTUDIO OBLIGADO AL ANALIZARSE EL FONDO DEL ASUNTO. Primera Sala de la SCJN. Tesis 1a./J.

## IV. Conclusiones

La facultad de atracción conferida al INAI por disposición constitucional y cuyo desarrollo en materia de protección de datos personales en posesión de los sujetos obligados se realiza a través de esta ley general, debe considerarse en cualquier caso, a pesar de su carácter discrecional, como un medio verdaderamente excepcional y sujeto a límites dados por el contenido y alcance de los criterios de interés y trascendencia. Este énfasis en la excepcionalidad de su ejercicio se explica no sólo por su carácter disruptivo en el régimen de distribución de competencias propias del federalismo, sino porque, además, su ejercicio priva de una posible instancia adicional a los recurrentes (los titulares de los datos personales o sus representantes) a través del recurso de inconformidad.

De hecho, la construcción jurisprudencial de la Corte Suprema en torno al ejercicio de la facultad de atracción ha puesto especial cuidado en subrayar su concepción como medio excepcional y en establecer los alcances de sus requisitos de procedencia a fin de evitar la arbitrariedad. Todo lo cual no obsta para reconocer que su previsión en la Norma Fundamental era necesaria para alcanzar el objetivo de generar criterios y estándares comunes de protección de datos personales en todo el país.

## Referencias

DOF. (2014). Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, *Diario Oficial de la Federación*. [Archivo PDF]. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_215_07feb14.pdf

DOF. (2015). Ley General de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*.

DOF. (2016). Ley Federal de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (enero 2018). Acuerdo mediante el cual se aprueba reformar los artículos 2, fracciones II, III, V, VI, IX, X, XII, XIII, XIV, XV y XVI; 4; 6; 9, fracciones II, incisos A y B, y XII; 11, fracción III; 12, apartado A, fracción III, y apartado C, fracción II, y 13 de los Lineamientos Generales para que el Instituto Nacional de Transparencia, Acceso a

24/2013, *Semanario Judicial de la Federación y su Gaceta*, Décima Época, Libro XVIII, Tomo 1, marzo de 2013, p. 400.

la Información y Protección de Datos Personales ejerza la facultad de atracción, *Diario Oficial de la Federación*.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (febrero 2017). Acuerdo mediante el cual se aprueban los nuevos Lineamientos generales para que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ejerza la facultad de atracción, *Diario Oficial de la Federación*.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (marzo 2016). Acuerdo mediante el cual se aprueban los Lineamientos generales para que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ejerza la facultad de atracción, así como los procedimientos internos para la tramitación de la misma, *Diario Oficial de la Federación*.

Suárez, A. (2017). "Usos e interpretación de la facultad de atracción en el juicio de amparo por la SCJN", en Ferrer Mac-Gregor, Eduardo y Herrera, Alonso (Coords.), *El juicio de amparo en el centenario de la Constitución mexicana de 1917. Pasado, Presente y Futuro*, Tomo I. México: Instituto de Investigaciones Jurídicas de la UNAM.

Suprema Corte de Justicia de la Nación. (diciembre 1996). Tesis P.CXLVIII/96, *Semanario Judicial de la Federación y su Gaceta*, Novena Época, Tomo IV, p. 109.

Suprema Corte de Justicia de la Nación. (octubre 2006). Tesis jurisprudencial 2a./J. 143/2006, *Semanario Judicial de la Federación y su Gaceta*, Novena Época, Tomo XXIV, p. 335.

Suprema Corte de Justicia de la Nación. (abril 2008). Tesis jurisprudencial 1a./J. 27/2008, *Semanario Judicial de la Federación y su Gaceta*, Novena Época, Tomo XXVII, p. 150.

Suprema Corte de Justicia de la Nación. (marzo 2013). Tesis jurisprudencial 1a./J. 24/2013, *Semanario Judicial de la Federación y su Gaceta*, Décima Época, Libro XVIII, Tomo 1, p. 400.

# CAPÍTULO V
# DEL RECURSO DE REVISIÓN EN MATERIA DE SEGURIDAD NACIONAL

***Artículo 139.*** *El Consejero Jurídico del Gobierno Federal podrá interponer recurso de revisión en materia de seguridad nacional directamente ante la Suprema Corte de Justicia de la Nación, cuando considere que las resoluciones emitidas por el Instituto ponen en peligro la seguridad nacional.*

*El recurso deberá interponerse durante los siete días siguientes a aquél en el que el organismo garante notifique la resolución al sujeto obligado. La Suprema Corte de Justicia de la Nación determinará, de inmediato, en su caso, la suspensión de la ejecución de la resolución y dentro de los cinco días siguientes a la interposición del recurso resolverá sobre su admisión o improcedencia.*

***Artículo 140.*** *En el escrito del recurso, el Consejero Jurídico del Gobierno Federal deberá señalar la resolución que se impugna, los fundamentos y motivos por los cuales considera que se pone en peligro la seguridad nacional, así como los elementos de prueba necesarios.*

***Artículo 141.*** *La información reservada o confidencial que, en su caso, sea solicitada por la Suprema Corte de Justicia de la Nación por resultar indispensable para resolver el asunto, deberá ser mantenida con ese carácter y no estará disponible en el Expediente, salvo en las excepciones previstas en el artículo 120 de la Ley General de Transparencia y Acceso a la Información Pública.*

*En todo momento, los Ministros deberán tener acceso a la información clasificada para determinar su naturaleza, según se requiera. El acceso se dará de conformidad con la normatividad previamente establecida para el resguardo o salvaguarda de la información por parte de los sujetos obligados.*

***Artículo 142.*** *La Suprema Corte de Justicia de la Nación resolverá con plenitud de jurisdicción, y en ningún caso, procederá el reenvío.*

***Artículo 143.*** *Si la Suprema Corte de Justicia de la Nación confirma el sentido de la resolución recurrida, el sujeto obligado deberá dar cumplimiento en los términos que establece la disposición correspondiente de esta Ley.*

*En caso de que se revoque la resolución, el Instituto deberá actuar en los términos que ordene la Suprema Corte de Justicia de la Nación.*

## COMENTARIO

**Michael G. Núñez Torres y Alonso Cavazos Guajardo Solís**

### I. Antecedentes

En los artículos 139 a 143 de la LGPDPPSO se contemplan las normas procesales del recurso de revisión en materia de seguridad nacional, un medio de impugnación de gran trascendencia para el constitucionalismo mexicano porque constituye una de las dimensiones del encuentro de dos preocupaciones fundamentales del Estado: la protección de datos personales, consagrada en la fracción II del artículo 6º de la CPEUM, y la seguridad nacional, reconocida en múltiples disposiciones de rango constitucional, entre las cuales resaltan los artículos 16, párrafo segundo; 20, apartado B, fracción V y 35, fracción VIII, numeral 3º de la propia CPEUM, así como también una vertiente del control constitucional de los actos de los poderes públicos, en este caso el órgano garante, con lo cual se asegura la supremacía constitucional en aquel punto de encuentro.

### II. Relevancia temática y contexto

En particular, conviene destacar que la seguridad, un presupuesto existencial para el Estado, tiene diferentes categorías que, por su trascendencia, requiere un tratamiento diferenciado. Así, la seguridad nacional es definida por el artículo 3º de la Ley de Seguridad Nacional como “las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano”, poniéndose de manifiesto la trascendencia de ésta para el derecho constitucional porque su tutela específica consiste en la integridad, estabilidad y permanencia del Estado. La génesis de la seguridad nacional se encuentra en el pacto federal, lo que refleja una protección integral al Estado, a los derechos fundamentales y a la división de poderes. El alcance de esta definición permite diferenciarla de otras categorías de la seguridad, como la seguridad pública que, en términos del artículo 2° de la Ley General del Sistema Nacional de Seguridad Pública, se encamina a salvaguardar la integridad y los derechos de las personas

y a preservar las libertades, el orden y la paz públicos. Esto implica que ambas están muy relacionadas, además con la seguridad jurídica, dado que en el fondo son elementos integrantes de un elemento teleológico del Estado: la seguridad. Sin embargo, sus fines específicos permiten establecer una regulación propia y diferenciada, como en este caso lo constituye el recurso de revisión en materia de seguridad nacional, que no tiene una institución procesal similar en lo que respecta a la seguridad pública.

La seguridad nacional ha sido particularmente problemática en América Latina porque su concepto se relaciona con una profunda carga ideológica que lo asocia a políticas de represión contrarias a los derechos humanos con el pretexto de la lucha contra los enemigos externos e internos del Estado y, a pesar de que en el siglo XXI las constituciones han legitimado este concepto reformulándolo sobre la base de los principios democráticos[281] del Estado constitucional, es un hecho que la tentación autoritaria aparece en el momento de que los gobiernos quieren trasgredir las limitaciones que al poder suponen los derechos humanos. Cobra relevancia que los arquetipos conceptuales de la seguridad nacional presentan dos modelos claramente diferenciados: el de los Estados Unidos de América, basado en la defensa exterior y la guerra preventiva, mientras que el modelo europeo se centra en la defensa nacional y de los valores democráticos,[282] no obstante, en ambos casos se encuentra latente el riesgo que mencionamos acerca de la utilización de esta cláusula teleológica del Estado como justificación para vulnerar los derechos humanos, en el caso que nos interesa, el derecho a la protección de datos personales.

Esta invitación a participar en tan destacada obra colectiva mediante la elaboración de un capítulo que analice de modo sumario el referido recurso de revisión en materia de seguridad nacional, supone un gran honor para quienes somos los autores de este capítulo, no sólo por la admiración y respeto que profesamos a quienes coordinan y participan en esta obra colectiva, sino también porque ese medio de impugnación responde más a una problemática del derecho constitucional, consistente en la tensión de las garantías de libertad y las de seguridad (en este caso representadas, respectivamente, por la protección de datos personales y por la seguridad nacional), lo cual hace idóneo abordarlo desde aquella rama de la ciencia jurídica y no a la luz del derecho procesal que se enfoca más en un análisis de la competencia, los sujetos legitimados, la acción y los efectos de la sentencia.

---

[281] Centro de Acceso a Archivos e Información Pública y Centro de Estudios para la Libertad de Expresión y Acceso a la Información de la Facultad de Derecho de la Universidad de Palermo. (2012). *Seguridad Nacional y Acceso a la Información en América Latina: Estado de la situación y desafíos*, p. 15. [Archivo PDF]. Disponible en: http://www.palermo.edu/cele/pdf/NS-AI.pdf, [fecha de consulta: 7 de mayo 2018].

[282] *Ibíd.*, p. 16.

Ciertamente, este recurso incumbe al derecho constitucional y al derecho procesal, pero sus matices más sobresalientes e interesantes se encuentran en el campo de aquél, de manera que en este trabajo se habrá de realizar una descripción sistemática de las normas constitucionales y legales que lo regulan, analizándolas desde la perspectiva del derecho constitucional y, en particular, del derecho constitucional procesal que *grosso modo* se encarga del análisis de las garantías constitucionales de cualquier procedimiento.[283]

## III. Análisis del contenido

**1. Génesis constitucional del recurso.** Mediante la reforma constitucional número 174, publicada en el *Diario Oficial de la Federación* el 20 de julio de 2007, se consagró en la fracción II del artículo 6º de la CPEUM que la información referente a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes. No debemos perder de vista que la protección de datos personales surgió como una consecuencia de la sociedad tecnológica en la cual nos movemos y en la que los datos de las personas son susceptibles de un tratamiento diferenciado por parte de una variedad de personas de derecho público para fines diversos que constituyen el primer parámetro de control para la garantía del derecho a la autodeterminación informativa. No corresponde en este apartado señalar la diferencia entre autodeterminación informativa y protección de datos personales, pero sí vale la pena que se advierta el problema que surge en torno a la naturaleza de principio y de derecho fundamental con la que estas categorías se pueden abordar sin que exista ninguna incompatibilidad en tanto que obedecen a una lógica distinta, pero que da lugar a interpretaciones jurisprudenciales disímiles.[284]

Ahora bien, este derecho fundamental, cuyos principios debían establecerse en las normas secundarias en razón de la reserva de ley contemplada en la fracción II del artículo 6º de la CPEUM, en una primera etapa debía ser desarrollado por cada orden de gobierno de manera autónoma en sus respectivos ámbitos de atribuciones (la Federación en los supuestos contemplados en el artículo 73 de la CPEUM —incluido, desde luego, el previsto en la fracción XXIX-M, relativo a la capacidad del Congreso de la Unión de expedir leyes en materia de seguridad nacional— y las entidades federativas en las otras materias, en términos de la cláusula residual contemplada en el artículo 124), ante la inexistencia de alguna ley general que contemplara los mínimos de homogeneización de las leyes federales y locales relacionadas con la protección de datos personales. Así, en lo que atañe a la Federación, cuya competencia se relaciona con la seguridad nacional, en la Ley Federal de Transparencia y Acceso a la Información

[283] Fix-Zamudio, H. (2002). *Introducción al Derecho procesal constitucional*. México: FUNDAP, p. 27.
[284] Adinolfi, G. (2017). Autodeterminación Informativa, Consideraciones acerca de un principio General y un Derecho Fundamental. *Cuestiones Constitucionales. Revista Mexicana de Derecho Constitucional*, núm. 17, pp. 5-7.

Gubernamental sólo se contemplaba como excepción a la protección de los datos personales, que los mismos obraran en registros públicos o en fuentes de acceso público, supuesto en el cual no podían clasificarse como información confidencial, en términos de lo establecido en el artículo 18, fracción II y último párrafo; en tanto que la seguridad nacional aparecía inconexa a la protección de datos personales, ya que sólo constituía un elemento para clasificar la información como reservada cuando aquélla resultara comprometida (artículo 13, fracción I) o para no sujetar al Comité de Investigación y Seguridad Nacional a la existencia de un Comité de Transparencia (artículo 31) y en la Ley de Seguridad Nacional se estableció que son confidenciales los datos personales de los sujetos que proporcionen información (artículo 63) y que en ningún caso se divulgará información reservada que, a pesar de no tener vinculación con amenazas a la seguridad nacional o con acciones o procedimientos preventivos de las mismas, lesionen la privacidad, la dignidad de las personas o revelen datos personales (artículo 64).

Desde esa perspectiva, podemos afirmar que la reserva de ley contemplada en la fracción II del artículo 6º de la CPEUM no fue lo suficientemente desarrollada por la Legislatura federal, pues la restricción a la protección de datos personales se limitó tan sólo a los casos en que éstos obraran en registros públicos y en fuentes de acceso público, no así tratándose de la seguridad nacional, en la que sólo se tuteló la protección de los datos personales de los sujetos que proporcionaran información y la divulgación de información reservada que revelara esos datos. Esta reforma constitucional otorgó una protección más amplia del derecho de acceso a la información respecto de la brindada por la Convención Americana sobre Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos, tal como sostuvo la Primera Sala de la Suprema Corte de Justicia de la Nación (SCJN) en la ejecutoria relativa al amparo en revisión número 137/2012 (véanse párrafos 113 a 117), emitida el 6 de febrero de 2013, lo cual irradia también a la protección de datos personales.

Posteriormente, mediante la reforma constitucional número 187, publicada en el DOF el 1 de junio de 2009, se adicionó un segundo párrafo al artículo 16 de la CPEUM para efecto de establecer, entre otros aspectos, que toda persona tiene derecho a la protección de sus datos personales y que la ley establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional. Ambas reformas son muy destacables porque con ello se transitó, de manera tímida, a la protección de los datos personales, más de manera sectorial, dentro de ciertos textos legislativos, que como un derecho fundamental de rango constitucional,[285] de tal suerte que en la actualidad el ordenamiento jurídico mexicano cuenta con una legislación garantista que recoge en gran medida lo que ha sido la evolución del mismo en el derecho comparado.

[285] García, A. (2007). La Protección de Datos Personales: Derecho Fundamental del Siglo XXI. Un estudio comparado, *Boletín Mexicano de Derecho Comparado*, nueva serie, núm. 120, p. 745.

En este sentido, destaca la reforma constitucional número 215, publicada en el DOF el 7 de febrero de 2014, a través de la cual constitucionalmente se vinculó de manera sólida a la seguridad nacional al acceso a la información y a la protección de datos personales. Así, en esta reforma se efectuaron tres cambios de gran relevancia para el objeto de investigación:

a) Se modificó la fracción I del apartado A[286] del artículo 6º de la CPEUM para efecto de establecer que toda información en posesión de los sujetos obligados es pública, pudiendo reservarse temporalmente sólo por razones de interés público y seguridad nacional, en los términos que fijen las leyes.

b) Se adicionó una fracción VIII al apartado A del artículo 6º de la CPEUM, en cuyo párrafo séptimo se estableció que las resoluciones del organismo garante (el INAI) son vinculatorias, definitivas e inatacables para los sujetos obligados, y que el consejero jurídico del gobierno podrá interponer en contra de aquéllas recurso de revisión ante la SCJN, sólo cuando dichas resoluciones puedan poner en peligro la seguridad nacional conforme a la ley de la materia.

c) Se adicionó la fracción XXIX-S al artículo 73 de la CPEUM, para efecto de dotar al Congreso de la Unión de la facultad de expedir leyes generales reglamentarias que desarrollen los principios y bases en materia de transparencia gubernamental, acceso a la información y protección de datos personales en posesión de las autoridades, entidades, órganos y organismos gubernamentales de todos los órdenes de gobierno.

Esta reforma constitucional es producto de tres iniciativas, de las cuales destaca la presentada el 13 de septiembre de 2012 por senadoras y senadores integrantes de los grupos parlamentarios del Partido Revolucionario Institucional y del Partido Verde Ecologista de México, pues es la única en la que se plantea la incorporación del recurso de revisión en materia de seguridad nacional, exponiéndose al respecto lo siguiente:

> Sin embargo, la experiencia constitucional muestra contundentemente que, salvo en el caso de los tribunales constitucionales que se constituyen como órganos límites, toda facultad debe tener un contrapeso que permita resolver, de manera excepcional, casos que puedan implicar condiciones especialmente delicadas que afecten [o] puedan afectar [el] interés nacional. Por ello esta iniciativa propone establecer un recurso especial y excepcional que se sustanciará ante la Suprema Corte de Justicia de la Nación. Este recurso podrá iniciarse cuando el organismo garante

[286] Mediante reforma constitucional número 208, publicada en el *Diario Oficial de la Federación* el 11 de junio de 2013, se reformó el artículo 6º de la CPEUM para efecto de dividirlo en dos apartados, el primero de ellos relacionado con la transparencia, el acceso a la información y la protección de datos personales.

> determine divulgar una información que, a juicio de las autoridades responsables, pueda representar una amenaza directa y trascendente a la seguridad nacional. En el caso de que este conflicto se presentara, y con el propósito de contar con un mecanismo expedito que permita resolver una diferencia a este respecto, la ley deberá establecer un procedimiento que permita que éste sea resuelto de manera definitiva por la Suprema Corte de Justicia de la Nación. El máximo tribunal deberá hacer un juicio sobre si la materia controvertida en efecto cabe dentro del concepto de seguridad nacional, así como señalar en su resolución el alcance de la afectación y, en su caso, las modalidades de reserva de la información en cuestión.

El extracto recién transcrito pone de manifiesto que el recurso de revisión en materia de seguridad nacional fue ideado por el constituyente permanente con el objeto de impedir el acceso a información que constitucionalmente tiene el carácter de reservada por incidir en la seguridad nacional, pero no pareciera proteger datos personales ni excepcionar dicha protección. Empero, la norma constitucional aprobada no hace distingo entre el acceso a la información y la protección a datos personales, pues se refiere sólo a las resoluciones del organismo garante que puedan poner en peligro la seguridad nacional, siendo que éstas pueden emitirse en esos ámbitos. Quizá por ello es que, pese a que ese recurso estaba llamado a regir —como lo hace— en materia de acceso a la información, también fue incorporado en la LGPDPPSO (artículos 139 a 143), prácticamente en los mismos términos en que se establece en los artículos 189 a 193 de la diversa Ley General de Transparencia y Acceso a la Información Pública. Pero debemos estar conscientes de que si bien se trata de dos recursos con el mismo cauce procesal, su teleología es totalmente distinta, pues mientras el contemplado en la Ley General de Transparencia tiende a impedir el acceso a información relacionada con la seguridad nacional, el previsto en la LGPDPPSO busca excepcionar la protección de datos personales en ese ámbito, reflejando con ello la tensión entre las dos instituciones, esto es, la protección de datos personales y la seguridad nacional, cobrando particular relevancia que la autodeterminación —reflejada en aquel derecho— no es ilimitada, teniendo gran elocuencia lo afirmado por el profesor Benda[287] en el sentido de que:

> Cuando un determinado comportamiento es perjudicial, no tiene por qué ser aceptado. Es legítima la protección de terceros o de la generalidad ante exhibiciones agresivas, molestas o incluso peligrosas (por ejemplo, para la juventud). Lo importante es tal protección, no la idea de que alguien haya de ser protegido contra sí mismo o contra una concepción dudosa de su dignidad.

[287] Benda, E. (2001). "Dignidad humana y derechos de la personalidad", en López Pina, A. (Ed.), *Manual de Derecho constitucional*. Madrid-Barcelona, España: Marcial Pons, p. 144.

La importancia de este medio de impugnación radica en la posibilidad de que el gobierno federal, a través de su consejero jurídico, cuestione ante la SCJN las decisiones de un órgano constitucional autónomo en el supuesto de que, a su parecer, puedan poner en riesgo la seguridad nacional. Partiendo de que el organismo garante está llamado, naturalmente, a proteger los datos personales, este medio de impugnación constitucional tiende a cuestionar las resoluciones en que se efectúe esa protección aun sobre la seguridad nacional, que conforme se verá, es una limitante legalmente reconocida al derecho a la protección de datos personales. Se trata de una institución que guarda ciertos paralelismos con el recurso de revisión contemplado en la fracción III del artículo 104 de la CPEUM, al permitir a ciertos sujetos de derecho público impugnar actos que no podrían controvertir a través del juicio de amparo, pero se distingue de éste en razón de que tiene un bien jurídico tutelado con un alto grado de especificidad, esto es, la seguridad nacional, mediante la cual se protegen diversos derechos fundamentales de los individuos en general, así como la estabilidad del Estado que, por sí mismo, es un medio eficiente para garantizar cualquier derecho fundamental.

Visto a la luz del principio de división de poderes, el recurso de revisión en materia de seguridad nacional es un importante contrapeso a cargo del Tribunal constitucional mexicano frente al peso específico del organismo garante, consistente en proteger los datos personales de los individuos, y desde la perspectiva de los derechos fundamentales, constituye un mecanismo que permite a nuestro Tribunal constitucional ponderar, caso por caso, si debe prevalecer el derecho constitucional a la protección de datos personales o la seguridad nacional, mediante la cual se protegen otros derechos tan relevantes como la vida, la salud, la integridad física y la seguridad.

Conviene destacar al respecto que el hecho de que la legislación general que regula la protección de datos personales esté enmarcada dentro de una serie de principios hace que el derecho requiera de una configuración jurisprudencial que atiende a las contingencias propias de cada caso, ya que, a pesar de lo detallado que ha tratado de ser el legislador, es un hecho que, como dice Lucas Murillo de la Cueva[288] refiriéndose al caso europeo, se trata de:

> Principios y tutela judicial que son especialmente importantes en un contexto en el que cada día se aprecia que la protección de datos debe extenderse a nuevos ámbitos —las telecomunicaciones, la videovigilancia, los servicios de la llamada sociedad de la información, el mundo de Internet— y a nuevos peligros, como los que pueden deparar las llamadas etiquetas inteligentes, los chips incorporados a personas, los brazaletes electrónicos, el uso de datos biométricos como mecanismos de seguridad en la identificación de individuos […].

[288] Murillo de la Cueva, P. (2008). "El derecho a la autodeterminación informativa y la protección de datos personales", *Azpilcueta*, núm. 20, pp. 43-58.

> En estos casos, en tanto se diseñan y aprueban las normas necesarias para prevenirlos o impedirlos, es en la aplicación judicial de los principios en donde residirá una de las principales líneas de defensa.

En el mismo sentido, el manejo de los datos personales es consecuencia del fenómeno de la globalización y de la revolución tecnológica con la cual viene aparejado, en este sentido, como bien afirma Remolina Angarita:[289]

> Para los Estados, es recurrente justificar la transferencia internacional de datos por motivos de seguridad pública, seguridad nacional, investigaciones contra el terrorismo, labores de inteligencia militar o policial, cooperación judicial, cooperación internacional en general, protección de un interés del titular del dato, controles de inmigración, etc.

Esto supone un grado de dificultad muy grande en la configuración de los límites a este derecho que habrá de tener en cuenta la SCJN, en medio de la ampliación más grande que ha experimentado el catálogo de derechos fundamentales en la historia constitucional y la crisis del Estado del siglo XXI en razón de los ataques a las instituciones del Estado de derecho por parte de diversos enemigos de la democracia, la justicia constitucional está obligada a configurar y armonizar el derecho a la protección de datos y la seguridad nacional.

Por lo tanto, el recurso de revisión en materia de seguridad nacional es una institución constitucional procesal que beneficia a la supremacía de la CPEUM, pues permite controlar ciertos actos del organismo garante y fortalecer con ello los derechos fundamentales, no sólo del individuo cuyos datos personales habrían sido protegidos por el organismo garante, sino también del universo indeterminado de individuos que conforman la sociedad mexicana, así como los límites de los poderes públicos. Los avances en la tecnología hacen idóneo que el derecho a la protección de datos personales tenga su asidero en la fuente jurisprudencial y no necesariamente en la normativa, que no siempre habrá de estar a la par de la revolución tecnológica que vivimos, a la cual no son ajenos los derechos fundamentales ni la seguridad nacional.

**2. Vaciamiento legal de las normas constitucionales.** Partiendo de la relevancia constitucional de la seguridad nacional en los asuntos del conocimiento del organismo garante y de la reserva de ley en torno a las excepciones del derecho a la protección de datos personales, en el párrafo segundo del artículo 6 de la LGPDPPSO se establece que aquel derecho solamente se puede limitar por razones de seguridad nacional, en términos de la ley en la materia, disposiciones de orden público, seguridad y salud

[289] Remolina, N. (2010). "¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?" *International Law, Revista Colombiana de Derecho Internacional,* núm. 16, pp. 489-524.

públicas o para proteger los derechos de terceros, en tanto que el artículo 80 de la propia norma general señala que la obtención y tratamiento de datos personales por parte de los sujetos obligados competentes en instancias de seguridad, procuración y administración de justicia está limitada a aquellos supuestos y categorías de datos que resulten necesarios y proporcionales para el ejercicio de las funciones en materia de seguridad nacional, seguridad pública o para la prevención o persecución de los delitos. El tratamiento que refiere la LGPDPPSO incluye, desde luego, la difusión o divulgación de datos personales, lo cual está particularmente justificado en seguridad nacional debido a la importancia de revelar datos que permitan identificar, por ejemplo, a un terrorista y actuar con la debida oportunidad para evitar la consumación o repetición de actos que afectan a la sociedad en general y cimbran las instituciones fundamentales del propio Estado, pero en estos casos, siguiendo los parámetros legales antes destacados, el organismo garante —y la SCJN, al resolver el recurso objeto de análisis— siempre debe efectuar una prueba del interés público, corroborar la conexión entre la información confidencial y el tema de interés público y la proporcionalidad entre la invasión a la intimidad ocasionada por la divulgación de aquella información y el interés público, tal como ha sostenido el Pleno de la SCJN en la ejecutoria emitida el 26 de mayo de 2015 para resolver la contradicción de tesis número 121/2014. Esta ponderación debe realizarse por el organismo garante en las resoluciones respectivas, de manera que las consideraciones correspondientes o la ausencia de las mismas constituyan el aspecto controvertido en el recurso de revisión contemplado en el párrafo séptimo de la fracción VIII del apartado A del artículo 6º de la CPEUM.

Ahora bien, destaca que el consejero jurídico del gobierno federal debe interponer directamente ante la SCJN el recurso de revisión en materia de seguridad nacional durante los siete días siguientes de que el INAI notifique la resolución impugnada al sujeto obligado (artículo 139 de la LGPDPPSO), con lo cual se atisba una primera limitante que pudiera afectar el derecho de impugnación que asiste al consejero jurídico del gobierno federal, ya que el detonante del plazo para impugnar consiste en un hecho totalmente ajeno a él y, en ese sentido, su impugnación está supeditada a que el sujeto obligado le remita de modo oportuno la resolución correspondiente. ¿Qué pasará cuando el sujeto obligado remita a la Consejería Jurídica del Gobierno Federal una resolución después de transcurrido aquel plazo? El recurso habrá de resultar improcedente por extemporáneo, lo cual rompe con el debido proceso legal como elemento racionalizador de las normas secundarias de carácter procesal, pero además, lo que se considera más grave, con el fin constitucional del propio medio de impugnación, consistente en que el sujeto de derecho público especializado en asuntos jurídicos recurra a la SCJN a plantear la falta o indebida ponderación entre seguridad nacional y protección de datos personales que efectúe el organismo garante. Debido al bien jurídico tutelado por este recurso constitucional, quizá habría sido conveniente determinar que,

en los casos relacionados con la seguridad nacional, el órgano garante notificara sus resoluciones directamente a la Consejería Jurídica del Gobierno Federal, pues con ello se le concedería un término efectivo para promover el recurso de revisión y cumplir a cabalidad los requisitos a que se contrae el artículo 140 de la LGPDPPSO, esto es, señalar en el escrito del recurso la resolución que se impugna, los fundamentos y motivos por los cuales considera que se pone en peligro la seguridad nacional y los elementos de prueba necesarios —o sea, los contemplados en el artículo 102, por ser ésta una disposición común a los recursos de revisión e inconformidad contemplados en la propia ley general—, siendo que éstos demuestran que no se está ante un recurso típico u ordinario en el que el ofrecimiento de pruebas está vedado o resulta excepcional. Otra arista de esta temática consiste en su incidencia en el régimen de responsabilidades al que está sujeto el consejero jurídico del gobierno federal, pues por una tardía o inexistente remisión por parte del sujeto obligado podría sujetarse a un procedimiento de responsabilidad administrativa, y si bien es claro que la presunción de inocencia que le asiste no podría desvirtuarse de manera sencilla, el simple sometimiento a un procedimiento le genera un agravio irreparable.

Por otra parte, el referido artículo 139 de la LGPDPPSO contempla en su párrafo segundo que la SCJN determinará de inmediato la suspensión de la ejecución de la resolución y dentro de los cinco días siguientes a la interposición del recurso resolverá sobre su admisión o improcedencia. La medida cautelar contemplada en este precepto es muy interesante, pues si partimos de que la resolución que naturalmente se impugnaría sería la que protege los datos personales sobre la seguridad nacional, evitando su obtención y tratamiento, la suspensión decretada por la SCJN tendría como efecto permitir que el sujeto obligado continúe obteniendo y tratando datos personales, con lo cual se da mayor preeminencia —al menos cautelar— a la seguridad nacional frente a la protección de los datos personales, beneficiándose así al colectivo frente al individuo.

Otro aspecto que resulta muy interesante consiste en que en el recurso de revisión en materia de seguridad pública no está contemplado, de modo expreso, el respeto a la garantía de audiencia que debiera asistir al individuo cuyos datos personales son materia de la obtención o del tratamiento debatido ante el INAI, habida cuenta que, de conformidad con la LGPDPPSO, luego de la admisión del recurso la SCJN debe recabar los medios probatorios correspondientes —incluida la información reservada o confidencial referida en el artículo 141— y resolver el asunto con plenitud de jurisdicción, sin que en ningún caso proceda el reenvío (artículo 142). No pasa inadvertido que el artículo 9 de la LGPDPPSO contempla que a falta de disposición expresa en esa norma general se aplicarán de manera supletoria el Código Federal de Procedimientos Civiles y la Ley Federal de Procedimiento Administrativo, sin embargo, los matices particulares del recurso de revisión en materia de seguridad nacional dificultan encontrar una norma que pueda aplicarse supletoriamente en este aspecto.

Lo anterior es relevante porque los efectos de la resolución emitida por la SCJN podrían significar que, en el ámbito de la seguridad nacional, se le restrinja o prive definitivamente de su derecho constitucional a la protección de datos personales, razón por la cual, bajo los más básicos estándares doctrinales y jurisprudenciales del derecho a la audiencia, debería dársele vista para efecto de que, previo al potencial acto privativo, manifieste lo que a su derecho convenga, así como permitirle a las partes la formulación de alegatos una vez que se han desahogado las pruebas que ofrecieron. Seguramente la SCJN habrá de ordenar esa vista partiendo de su propia jurisprudencia en la que reconoce que aun las autoridades administrativas están constreñidas a respetar la garantía de previa audiencia aunque la ley correspondiente no la establezca (170392, 2a./J. 16/2008); sin embargo, la circunstancia de que no esté contemplada en la norma general impregna a ésta de un vicio de inconstitucionalidad que termina por fragmentar las prerrogativas constitucionales que son materia de debate, esto es, el derecho de protección de datos personales y la seguridad nacional.

La ausencia de vista al individuo que pudiera resultar afectado en su derecho a la protección de datos personales es diametralmente opuesta a las garantías específicas del debido proceso legal, incluida, desde luego, la de previa audiencia. Aunque también constituye una flagrante violación al principio de igualdad procesal, puesto que coloca al consejero jurídico del gobierno federal en una posición procesal privilegiada en la medida que la SCJN sólo escuchará sus argumentos y recibirá sus pruebas, teniendo una visión unilateral de un conflicto en el que la pugna se ciñe a la ponderación del derecho a la protección de datos personales y de la seguridad nacional, con lo cual se pone en entredicho también su imparcialidad.

## IV. Conclusiones

Si bien está claro que el INAI es un órgano constitucional autónomo, no se puede perder de vista que sus actos son susceptibles de revisión constitucional, precisamente a través de los mecanismos que, para tal efecto, contempla la CPEUM, como el recurso de revisión en materia de seguridad nacional.

La consagración del recurso de revisión en materia de seguridad nacional obedeció a una lógica protectora del derecho a la protección de datos personales que constituyen información confidencial para efectos de las solicitudes de acceso a la información, sin embargo, el legislador permitió que también se erigiera como un mecanismo garante de la seguridad nacional, entendida como una restricción a la protección de datos personales. Así, se revela una tensión entre el derecho a la protección de datos personales y la seguridad nacional,

ambos de rango constitucional, que es dirimida a través de una vía procesal casi idéntica, pero con fines diferenciados según se trate de las legislaciones generales correspondientes.

La LGPDPPSO desarrolla el recurso de revisión en materia de seguridad nacional, el cual constituye una novedad significativa por parte del legislador en virtud de la concepción (un tanto heterodoxa) con la cual se define el propio recurso, las relaciones que los sujetos procesales van a tener dentro del mismo y la concreción de las garantías del debido proceso que deben ser llevadas a cabo por la jurisdicción constitucional.

Si bien se trata de un recurso de gran relevancia, se vislumbra difícil su concreción en razón de que resultaría sumamente excepcional que un individuo, cuyos datos personales son obtenidos o tratados en razón de la seguridad nacional, acuda ante el órgano garante a protegerlos. Más excepcional resulta, que el órgano garante determine hacerlo y el consejero jurídico del gobierno promueva el recurso de revisión objeto de análisis.

## Referencias

Adinolfi, G. (2007). Autodeterminación Informativa, Consideraciones acerca de un principio General y un Derecho Fundamental, *Cuestiones Constitucionales. Revista Mexicana de Derecho Constitucional*, núm. 17, (julio-diciembre), pp. 3-29.

Benda, E. (2001). “Dignidad humana y derechos de la personalidad”, en López Pina, Antonio (Ed.), *Manual de Derecho constitucional.* Madrid-Barcelona, España: Marcial Pons, p. 117 a 144.

Centro de Acceso a Archivos e Información Pública y Centro de Estudios para la Libertad de Expresión y Acceso a la Información de la Facultad de Derecho de la Universidad de Palermo. (2012). *Seguridad Nacional y Acceso a la Información en América Latina: Estado de la situación y desafíos*. [Archivo PDF]. Disponible en: http://www.palermo.edu/cele/pdf/NS-AI.pdf, [fecha de consulta: 8 de mayo 2018].

Fix-Zamudio, H. (2002). *Introducción al Derecho procesal constitucional.* México: FUNDAP.

García, A. (septiembre-diciembre 2007). La Protección de Datos Personales: Derecho Fundamental del Siglo XXI. Un estudio comparado, *Boletín Mexicano de Derecho Comparado*, nueva serie, núm. 120, pp. 743-778.

Murillo de la Cueva, P. (2008). El derecho a la autodeterminación informativa y la protección de datos personales. *Azpilcueta*, núm. 20, pp. 43-58.

Remolina, N. (2010). ¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?. *International Law, Revista Colombiana de Derecho Internacional*, núm. 16, pp. 489-524.

# CAPÍTULO VI
# DE LOS CRITERIOS DE INTERPRETACIÓN

***Artículo 144.*** *Una vez que hayan causado ejecutoria las resoluciones dictadas con motivo de los recursos que se sometan a su competencia, el Instituto podrá emitir los criterios de interpretación que estime pertinentes y que deriven de lo resuelto en los mismos, conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable.*

*El Instituto podrá emitir criterios de carácter orientador para los Organismos garantes, que se establecerán por reiteración al resolver tres casos análogos de manera consecutiva en el mismo sentido, por al menos dos terceras partes del Pleno del Instituto, derivados de resoluciones que hayan causado estado.*

***Artículo 145.*** *Los criterios se compondrán de un rubro, un texto y el precedente o precedentes que, en su caso, hayan originado su emisión.*

*Todo criterio que emita el Instituto deberá contener una clave de control para su debida identificación.*

## COMENTARIO

**Olivia Andrea Mendoza Enríquez**

### I. Antecedentes

La facultad del INAI para emitir criterios de interpretación encuentra su origen en la LFTAIPG de 2002, ya que en este instrumento se facultaba al entonces Instituto Federal de Acceso a la Información (ahora INAI) para interpretar en el orden administrativo la citada ley.[290]

[290] Artículo 37. El Instituto tendrá las siguientes atribuciones:
I. Interpretar en el orden administrativo esta Ley, de conformidad con el Artículo 6; […].

En el mismo sentido, la facultad del INAI para emitir criterios de interpretación tiene otro antecedente importante en la LFPDPPP de 2010,[291] ya que el Congreso de la Unión lo designó como autoridad garante del derecho a la protección de datos personales en posesión del sector privado.[292]

En este sentido, el artículo 39 de la LFPDPPP dota de facultades al Instituto para emitir los criterios y recomendaciones para garantizar el pleno derecho a la protección de datos personales.[293]

Finalmente, la LGTAIP de 2015, terminó de establecer las bases a considerar para la emisión de criterios de interpretación por parte del INAI, particularmente al establecer que una vez que hayan causado ejecutoria las resoluciones dictadas en los recursos de revisión que se sometan a competencia del Pleno, el Instituto podrá emitir los criterios de interpretación que estime pertinentes y que deriven de lo resuelto en dichos asuntos, asimismo, el INAI podrá emitir criterios de carácter orientador para los organismos garantes locales, que se establecerán por reiteración, al resolver tres casos análogos de manera consecutiva en el mismo sentido, por al menos dos terceras partes del Pleno del Instituto y derivados de resoluciones que hayan causado estado.[294]

Como requisito para la composición de criterios se prevé que deben incluir rubro, texto y precedente que en su caso hayan originado la emisión.[295]

## II. Relevancia temática y contexto

Los criterios de interpretación formulados por el INAI derivan del análisis que, sobre un tema determinado (acceso a la información o protección de datos personales), ha realizado el Pleno de dicho Instituto, los cuales son de aplicación obligatoria para los sujetos obligados del ámbito federal y no vinculatorios para los organismos garantes de las entidades federativas, ya que los criterios de interpretación, en este caso, tienen un carácter orientador.

---

[291] La Ley Federal de Protección de Datos Personales en Posesión de los Particulares modificó la denominación del que antes era el Instituto Federal de Acceso a la Información Pública, para nombrarlo Instituto Federal de Acceso a la Información Pública y Protección de Datos, a partir de la entrada en vigor de la citada ley, el 6 de julio de 2010.

[292] Ornelas, L. (2013). "Características del modelo de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento", en Ornelas, L. y Piñar, J. (Coords.), *La protección de datos personales en México*. México: Tirant Lo Blanch, pp. 128-129.

[293] "Artículo 39. El Instituto tiene las siguientes atribuciones:
[…]
II. Interpretar en el ámbito administrativo la presente Ley.
[…]
IV. Emitir los criterios y recomendaciones, de conformidad con las disposiciones aplicables a esta Ley, para efectos de su funcionamiento y operación".

[294] Artículo 199 de la Ley General de Transparencia y Acceso a la Información Pública de 4 de mayo de 2015.

[295] Artículo 200 de la Ley General de Transparencia y Acceso a la Información Pública.

Como se verá más adelante, los artículos 144 y 145 de la LGPDPPSO refieren a la facultad del INAI, para emitir los criterios de interpretación que deriven de lo resuelto en los recursos de revisión de los que el Pleno conozca.

En este sentido, interpretar es la actividad de asignar sentido o significado a textos jurídicos, por ejemplo, artículos de una ley, fracciones de un reglamento, párrafos de una constitución, capítulos de un tratado. El producto de la actividad de interpretar un texto se expresa en palabras, frases y enunciados que llamamos enunciados interpretativos. El sentido de las palabras que expresan el significado del texto, se denomina interpretación.[296]

Los criterios de interpretación formulados por el INAI permiten que los sujetos obligados de la LGPDPPSO tengan mayores elementos para garantizar las disposiciones del derecho a la protección de datos personales.

Es importante señalar que los criterios de interpretación derivan de la identificación de un tema relevante para el derecho a la protección de datos personales, de la revisión de las resoluciones emitidas por el Pleno del Instituto y de la elaboración de un proyecto de criterio que tendrá que ser aprobado por el mismo Pleno.

Aunado a lo anterior, se debe precisar que los criterios de interpretación son distintos a las resoluciones emitidas por el Pleno del INAI, ya que, si bien estas últimas sustentan la emisión de criterios, podríamos estar ante situaciones de resoluciones dictadas dentro de recursos de revisión que no concluyan en la emisión de un criterio de interpretación.

Los criterios de interpretación que emite el Pleno del INAI no son atemporales, ya que cuentan con una vigencia determinada, por ejemplo, por la actualización en la regulación en la materia. En este sentido, actualmente existen dos momentos en la elaboración de criterios de interpretación: aquellos emitidos en el marco de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (2009-2014), que hoy día tienen carácter de históricos, y aquellos emitidos en el marco de la Ley General de Transparencia y Acceso a la Información Pública, a la Ley Federal de Transparencia y Acceso a la Información Pública y a la LGPDPPSO (2015-2017). Los criterios de interpretación con carácter de históricos sólo sirven como referencia para el tema tratado.

Por otro lado, los criterios de interpretación subsisten, siempre y cuando el Pleno del INAI, no emita una resolución distinta a lo que establecía el criterio.

[296] Rodríguez, G. (2013). *Interpretación conforme. Metodología para la enseñanza de la reforma constitucional en materia de derechos humanos*. México: Suprema Corte de Justicia de la Nación.

En caso de que un criterio resultara interrumpido por una postura del Pleno distinta, no podrá utilizarse más.[297]

A manera de conclusión de este apartado, podemos destacar que los criterios de interpretación permiten al operador del derecho a la protección de datos personales —en este caso, sujetos obligados de la ley—, conocer la postura que el Instituto adopta en situaciones previas y análogas a la que se pretende resolver.

## III. Análisis del contenido

El artículo 144 de la LGPDPPSO establece que una vez que hayan causado ejecutoria las resoluciones dictadas por el Pleno del INAI, con motivo de los recursos que se sometan a su competencia, el Instituto podrá emitir los criterios de interpretación que estime pertinentes y que deriven de lo resuelto en los mismos conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública y demás normativa aplicable.

El Instituto podrá emitir criterios de carácter orientador para los organismos garantes, los cuales se establecerán por reiteración al resolver tres casos análogos de manera consecutiva en el mismo sentido, por al menos dos terceras partes del Pleno del Instituto, derivados de resoluciones que hayan causado estado.

Por su parte, el artículo 145 de la citada ley establece que los criterios se compondrán de un rubro, un texto y el precedente o precedentes que, en su caso, hayan originado su emisión, y que todo criterio que emita el Instituto deberá contener una clave de control para su debida identificación. En este sentido, el rubro identifica al criterio, estableciendo con concisión, claridad y congruencia la esencia del mismo y proporcionando una idea sobre éste.[298]

Por su parte, el texto del criterio —como se ha dicho— deriva de las resoluciones en las que se interpretó de manera similar el derecho a la protección de datos personales, al emitir el pronunciamiento resolutivo.

Los precedentes se señalan al final de texto del criterio de interpretación con los números correspondientes al recurso de revisión y el nombre del sujeto obligado recurrido, así como el nombre del comisionado ponente en dicho recurso.

[297] Información disponible en: http://criteriosdeinterpretacion.inai.org.mx/Pages/default.aspx

[298] A efectos de la emisión de criterios, se deberá observar el Acuerdo mediante el cual se aprueban los Lineamientos para la emisión de criterios de interpretación del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, publicados en el *Diario Oficial de la Federación* el 3 de marzo de 2016.

Finalmente, se designará al criterio de interpretación un número específico, a fin de identificarlo, en el que se señalará número consecutivo y año en el que el Pleno del INAI lo aprobó.

Los criterios de interpretación en materia de protección de datos personales encuentran disposiciones relacionadas, no sólo en la legislación en materia de datos personales, sino en legislación en materia de acceso a la información, como es el caso del artículo 74, fracción III, inciso b, de la LGTAIP que establece que los órganos autónomos, entre ellos los organismos garantes del derecho de acceso a la información y la protección de datos personales, deberán poner a disposición del público y actualizar la información relativa a los criterios orientadores que deriven de sus resoluciones.

Resulta importante decir que la facultad de interpretación otorgada al INAI hace diferencia entre los criterios de interpretación y aquellos denominados orientadores, ya que los primeros son obligatorios para los sujetos de la ley y los segundos son recomendaciones para las entidades federativas. Esto a fin de salvaguardar el margen de apreciación de los estados, pero estableciendo bases mínimas, señaladas a través de una ley general.

En este sentido, la facultad concedida al INAI para emitir criterios de interpretación no vinculatorios, pero sí con carácter de orientadores, a las entidades federativas, es una facultad discutida en torno al ámbito de competencia del Instituto. Sin embargo, a partir de 2014, con la autonomía constitucional del mismo, se avala su competencia en asuntos descritos en la legislación para los tres órdenes de gobierno. Por ejemplo, la facultad de atracción en determinados recursos previstos en la Ley General de Transparencia y Acceso a la Información de 2015.

La facultad de emitir criterios orientadores podría considerarse un exceso de las facultades del órgano garante en el ámbito nacional, pero la experiencia desde la garantía, tanto del derecho de acceso a información como el de protección de datos personales en las entidades federativas, justifica la necesidad de contar con un estándar mínimo en la garantía de ambos derechos. En el mismo sentido, se deberá propiciar una estandarización en el ejercicio del derecho de protección de datos personales, ya que el riesgo de salvaguardar facultades como las de interpretación, a las entidades federativas, podría conllevar a una falta de hegemonía en el ejercicio y garantía de este derecho.

## IV. Conclusiones

Los criterios orientadores y de interpretación —como su nombre lo dice— sirven a los operadores del derecho a la protección de datos personales para conocer la postura del Pleno en situaciones similares que han resuelto. Sin embargo,

el derecho a la protección de datos personales es un derecho humano y, atendiendo a la reforma constitucional en materia de derechos humanos de 2011 y al principio pro persona, se deberán observar otros instrumentos para garantizarlo, como es el caso de las resoluciones de la Corte Interamericana de Derechos Humanos, tratados internacionales y otros instrumentos normativos reconocidos por el Estado mexicano.

Lo anterior se explica con las disposiciones del artículo 8 de la LGPDPPSO, el cual establece que la aplicación e interpretación de la citada ley se realizará conforme a lo dispuesto en la CPEUM, los tratados internacionales de los que el Estado mexicano sea parte, así como las resoluciones y sentencias vinculantes que emitan los órganos nacionales e internacionales especializados, favoreciendo en todo tiempo el derecho a la privacidad, la protección de datos personales y a las personas la protección más amplia. Para el caso de la interpretación, se podrán tomar en cuenta los criterios, determinaciones y opiniones de los organismos nacionales e internacionales en materia de protección de datos personales.

Es necesario decir que los criterios de interpretación y de orientación buscan, entre otras cosas, eliminar las asimetrías en la garantía del derecho a la protección de datos personales en posesión de sujetos obligados en los tres órdenes de gobierno.

## Referencias

DOF. (2015). Ley General de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*.

DOF. (2016). Ley Federal de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (marzo 2016). Acuerdo mediante el cual se aprueban los Lineamientos para la emisión de criterios de interpretación del Instituto Nacional de Transparencia, Acceso a la Información y Protección de datos Personales, *Diario Oficial de la Federación*.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2017), *Criterios de interpretación*. Disponible en: http://criteriosdeinterpretacion.inai.org.mx/Pages/default.aspx, [fecha de consulta: 8 de mayo 2018].

Ornelas, L. (2013). “Características del modelo de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento”, en Ornelas, L. y Piñar, J. (Coords.). *La protección de datos personales en México*. México: Tirant Lo Blanch, pp. 128-129.

Rodríguez, G. (2013). *Interpretación conforme. Metodología para la enseñanza de la reforma constitucional en materia de derechos humanos*. México: Suprema Corte de Justicia de la Nación.

# TÍTULO DÉCIMO

# FACULTAD DE VERIFICACIÓN DEL INSTITUTO Y LOS ORGANISMOS GARANTES

# CAPÍTULO ÚNICO
# DEL PROCEDIMIENTO DE VERIFICACIÓN

***Artículo 146.*** *El Instituto y los Organismos garantes, en el ámbito de sus respectivas competencias, tendrán la atribución de vigilar y verificar el cumplimiento de las disposiciones contenidas en la presente Ley y demás ordenamientos que se deriven de ésta.*

*En el ejercicio de las funciones de vigilancia y verificación, el personal del Instituto o, en su caso, de los Organismos garantes estarán obligados a guardar confidencialidad sobre la información a la que tengan acceso en virtud de la verificación correspondiente.*

*El responsable no podrá negar el acceso a la documentación solicitada con motivo de una verificación, o a sus bases de datos personales, ni podrá invocar la reserva o la confidencialidad de la información.*

***Artículo 147.*** *La verificación podrá iniciarse:*

*I. De oficio cuando el Instituto o los Organismos garantes cuenten con indicios que hagan presumir fundada y motivada la existencia de violaciones a las leyes correspondientes, o*

*II. Por denuncia del titular cuando considere que ha sido afectado por actos del responsable que puedan ser contrarios a lo dispuesto por la presente Ley y demás normativa aplicable, o en su caso, por cualquier persona cuando tenga conocimiento de presuntos incumplimientos a las obligaciones previstas en la presente Ley y demás disposiciones que resulten aplicables en la materia.*

*El derecho a presentar una denuncia precluye en el término de un año contado a partir del día siguiente en que se realicen los hechos u omisiones materia de la misma. Cuando los hechos u omisiones sean de tracto sucesivo, el término empezará a contar a partir del día hábil siguiente al último hecho realizado.*

*La verificación no procederá en los supuestos de procedencia del recurso de revisión o inconformidad previstos en la presente Ley.*

*La verificación no se admitirá en los supuestos de procedencia del recurso de revisión o inconformidad, previstos en la presente Ley.*

*Previo a la verificación respectiva, el Instituto o los Organismos garantes podrán desarrollar investigaciones previas, con el fin de contar con elementos para fundar y motivar el acuerdo de inicio respectivo.*

***Artículo 148.*** *Para la presentación de una denuncia no podrán solicitarse mayores requisitos que los que a continuación se describen:*

*I. El nombre de la persona que denuncia, o en su caso, de su representante;*

*II. El domicilio o medio para recibir notificaciones de la persona que denuncia;*

*III. La relación de hechos en que se basa la denuncia y los elementos con los que cuente para probar su dicho;*

*IV. El responsable denunciado y su domicilio, o en su caso, los datos para su identificación y/o ubicación;*

*V. La firma del denunciante, o en su caso, de su representante. En caso de no saber firmar, bastará la huella digital.*

*La denuncia podrá presentarse por escrito libre, o a través de los formatos, medios electrónicos o cualquier otro medio que al efecto establezca el Instituto o los Organismos garantes, según corresponda.*

*Una vez recibida la denuncia, el Instituto y los Organismos garantes, según corresponda, deberán acusar recibo de la misma. El acuerdo correspondiente se notificará al denunciante.*

***Artículo 149.*** *La verificación iniciará mediante una orden escrita que funde y motive la procedencia de la actuación por parte del Instituto o de los Organismos garantes, la cual tiene por objeto requerir al responsable la documentación e información necesaria vinculada con la presunta violación y/o realizar visitas a las oficinas o instalaciones del responsable, o en su caso, en el lugar donde estén ubicadas las bases de datos personales respectivas.*

*Para la verificación en instancias de seguridad nacional y seguridad pública, se requerirá en la resolución, la aprobación del Pleno del Instituto, por mayoría calificada de sus Comisionados, o de los integrantes de los Organismos garantes de las Entidades Federativas, según corresponda; así como de una fundamentación y motivación reforzada de la causa del procedimiento,*

*debiéndose asegurar la información sólo para uso exclusivo de la autoridad y para los fines establecidos en el artículo 150.*

*El procedimiento de verificación deberá tener una duración máxima de cincuenta días.*

*El Instituto o los organismos garantes podrán ordenar medidas cautelares, si del desahogo de la verificación advierten un daño inminente o irreparable en materia de protección de datos personales, siempre y cuando no impidan el cumplimiento de las funciones ni el aseguramiento de bases de datos de los sujetos obligados.*

*Estas medidas sólo podrán tener una finalidad correctiva y será temporal hasta entonces los sujetos obligados lleven a cabo las recomendaciones hechas por el Instituto o los Organismos garantes según corresponda.*

***Artículo 150.*** *El procedimiento de verificación concluirá con la resolución que emita el Instituto o los Organismos garantes, en la cual, se establecerán las medidas que deberá adoptar el responsable en el plazo que la misma determine.*

***Artículo 151.*** *Los responsables podrán voluntariamente someterse a la realización de auditorías por parte del Instituto o los Organismos garantes, según corresponda, que tengan por objeto verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la presente Ley y demás normativa que resulte aplicable.*

*El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles implementados por el responsable, identificar sus deficiencias, así como proponer acciones correctivas complementarias, o bien, recomendaciones que en su caso correspondan.*

## COMENTARIO

**Alessandra Barzizza y Mauricio Castillo**

### I. Antecedentes

La efectividad de los principios consagrados en esta ley general y el cumplimiento de las obligaciones previstas en la misma requieren de atribuciones para que los órganos garantes del derecho a la protección de datos personales estén en posibilidad de investigar, vigilar, comprobar y supervisar la actuación de los sujetos obligados respecto del tratamiento de los datos personales. A través del procedimiento de verificación, previsto en este capítulo, el legislador ha comprendido esta posibilidad, a fin de que las autoridades garantes del

derecho a la protección de datos personales puedan allegarse de elementos suficientes para investigar posibles actos ilegales,[299] o bien, para que los ciudadanos cuenten con los medios o mecanismos que les permitan iniciar una investigación en contra de los actos que violenten su derecho a la protección de datos personales.

Cabe advertir que si bien la reforma constitucional de 2014 en materia de transparencia y protección de datos personales amplía el espectro de sujetos obligados (bajo un régimen propio del sector público), el procedimiento de verificación no es una figura del todo nueva. Los Lineamientos de Protección de Datos Personales de 2005 ya preveían un mecanismo de supervisión, a través del cual, las dependencias y entidades de la Administración Pública Federal estaban obligadas a permitir a los servidores públicos del IFAI (ahora INAI) o a terceros previamente designados por éste, el acceso a los lugares en los que se encontraban y operaban los sistemas de datos personales, así como poner a su disposición la documentación técnica y administrativa de los mismos con el fin de supervisar el cumplimiento de las disposiciones jurídicas en la materia.[300]

Por lo que respecta al sector privado, la LFPDPPP de 2010 comprende, en su capítulo VIII, el procedimiento de verificación, mismo que tiene por finalidad vigilar el cumplimiento de su contenido normativo y de la normatividad que de ella se derive.[301] El cual, si bien cumple la misma función que el procedimiento de verificación previsto en la LGPDPPSO como medio de defensa de la legalidad, tiene algunas variantes en cuanto a su desarrollo y a las vías procesales correspondientes para su impugnación.

Por lo que hace al procedimiento de verificación en esta ley general, el artículo 146 dispone que, tanto el INAI como los organismos garantes, en el ámbito de sus competencias, tendrán la atribución de vigilar y verificar el cumplimiento de las disposiciones de la ley y las que emanen de la misma. Para esos efectos, los responsables del tratamiento (sujetos obligados) no podrán negar el acceso a la documentación solicitada, a sus bases de datos personales, ni invocar la reserva o confidencialidad de la información. No obstante, el INAI y los organismos garantes deberán guardar el deber de confidencialidad respecto de la misma.

---

[299] El Ministerio Público, en otro ámbito, cumple funciones de investigación. Su principal actividad, al decir de Fix-Zamudio, consiste en la defensa de la legalidad, ya sea en una investigación o en una acusación. Cfr. Fix-Zamudio, H. (1978). La función constitucional del Ministerio Público, *Anuario Jurídico*, vol. V, Instituto de Investigaciones Jurídicas de la UNAM.

[300] Cfr. DOF. (septiembre 2005). Lineamiento Cuadragésimo tercero de los Lineamientos de Protección de Datos Personales, *Diario Oficial de la Federación*.

[301] Estas atribuciones de supervisión, inspección, vigilancia o verificación también fueron adoptadas por otras legislaciones emitidas en algunas entidades federativas y el entonces llamado Distrito Federal, con algunas variantes.

## II. Relevancia temática y contexto

La reforma constitucional de 2011 en materia de derechos humanos ha impactado de manera sustantiva la labor de todas las autoridades e instituciones del país, independientemente de su jerarquía o del orden (federal, estatal o municipal) al que pertenecen. A través de la misma se precisa la distinción entre los derechos humanos (como el derecho a la protección de datos personales) y las garantías previstas para su protección.[302] Mediante esta distinción se establecieron las obligaciones que las autoridades e instituciones del Estado mexicano deben cumplir para asegurar la aplicación efectiva de los derechos humanos. Estas obligaciones se encuentran comprendidas en el artículo 1º de la CPEUM, el cual establece que "[…] todas las autoridades, en el ámbito de sus competencias, tienen la obligación de promover, respetar, proteger y garantizar los derechos humanos […]".

Si bien el texto constitucional anteriormente citado no dice demasiado en torno a las obligaciones estatales ahí establecidas, éstas no son meros postulados. Para poder comprender el vínculo que existe entre estas obligaciones y el derecho a la protección de datos personales es necesario exponer y explicar, de manera breve, su contenido y alcance, así como la manera en la que se relacionan con el procedimiento de verificación que el INAI se encuentra facultado para realizar con base en esta ley general.

1) **Obligación de promover.** Esta obligación se refiere a que es responsabilidad del Estado que las personas conozcan sus derechos, cómo ejercerlos mejor y los mecanismos con los que cuentan para exigir su cumplimiento u obtener reparación, en caso de que existan violaciones a los mismos.[303]

2) **Obligación de respetar.** Esta obligación implica que el Estado debe abstenerse de realizar actos que resulten violatorios a los derechos humanos. Lo anterior no supone que el Estado no puede adoptar medidas que restrinjan algún derecho, sino que la finalidad de estas restricciones debe ser siempre el cumplimiento de las propias obligaciones del Estado en relación con otros derechos y no el ejercicio ilegal o arbitrario de su potestad.[304]

---

[302] Previo a la reforma de 2011 el Capítulo Primero del Título Primero de la Constitución Política de los Estados Unidos Mexicanos se denominaba De las Garantías Individuales. Hoy en día se denomina De los Derechos Humanos y sus Garantías. Asimismo, en el propio texto del artículo 1º de la Constitución se distingue expresamente entre los derechos humanos y las garantías que existen para su efectiva protección e implementación.

[303] Salazar, P. (Coord.). (2014). *La reforma constitucional sobre derechos humanos. Una guía conceptual.* México: Instituto Belisario Domínguez, Senado de la República, pp. 111-131.

[304] *Ibíd.*, p. 115.

3) **Obligación de proteger.** Esta obligación implica que el Estado debe tomar medidas para impedir que las autoridades, instituciones gubernamentales o los particulares (bajo ciertos supuestos) violen los derechos de las personas.

   Las medidas específicas que los Estados deben adoptar en este sentido varían dependiendo de cada materia, sin embargo, el cumplimiento con esta obligación generalmente se analiza con base en un criterio de razonabilidad. Se trata de una obligación de medios y no de resultados, ya que resulta materialmente imposible que un Estado impida la realización de todas las conductas violatorias de derechos que se suscitan dentro de su territorio, especialmente cuando se trata de acciones realizadas por particulares.[305]

4) **Obligación de garantizar.** Esta obligación se refiere a que el Estado debe encargarse de implementar las condiciones y los medios institucionales para que las personas puedan ejercer y exigir, de manera efectiva y por sí mismos, sus derechos humanos.[306]

El cumplimiento de estas obligaciones por parte del Estado permite que los derechos humanos tengan un impacto material en la vida de las personas que se encuentran sujetas a su jurisdicción. De lo contrario, estos derechos terminarían siendo meros conceptos inertes enunciados en el texto constitucional. Detrás de cada violación de un derecho humano se encuentra el incumplimiento, por parte del Estado, con una de estas obligaciones, mientras que detrás de cada goce efectivo de un derecho se encuentra el cumplimiento con alguna de ellas.

Precisamente, el procedimiento de verificación, sea que inicie como una facultad de oficio o a instancia de parte a través de una denuncia, constituye un mecanismo para dar cumplimiento a dichas obligaciones. El Estado cumple con la obligación de salvaguardar el derecho a la protección de datos personales cuando inicia, de oficio, dicho procedimiento. Lo anterior se debe a que, mediante este procedimiento, el INAI podría llegar a identificar prácticas u omisiones por parte de los responsables del tratamiento de datos personales, que eventualmente podrían derivar en violaciones a este derecho humano. Asimismo, en caso de identificar que estas acciones u omisiones ya han derivado en violaciones, el INAI podrá sancionar y ordenar la implementación de medidas para evitar que se repita en el futuro, lo cual también es una manera de prevenirlas.

Por otro lado, la obligación del Estado de “garantizar” el derecho a la protección de datos personales se satisface cuando el procedimiento de

[305] *Ibíd.*, p. 116.
[306] *Idem.*

verificación se inicia a través de una denuncia. Lo anterior se debe a que el proceso de denuncia implica el establecimiento de un mecanismo para que los titulares puedan exigir el cumplimiento y respeto de su derecho humano a la protección de datos personales.

El hecho de que el procedimiento de verificación se identifique como una forma de proteger y garantizar el derecho a la protección de datos personales no quiere decir que éste sea el único medio a través del cual el Estado cumple con esta obligación, existen muchos otros mecanismos de cumplimiento de estas obligaciones, por ejemplo, el recurso de inconformidad, específicamente por lo que respecta al ejercicio de los derechos ARCO.

## III. Análisis del contenido

**1. Procedencia del procedimiento de verificación.** El artículo 147 de la LGPDPPSO en sus fracciones I y II establece que el procedimiento de verificación podrá iniciarse de oficio o a petición de parte "cuando el Instituto o los organismos garantes cuenten con indicios que hagan presumir fundada y motivada[mente] la existencia de violaciones a las leyes correspondientes", o bien, cuando el titular considere que ha sido afectado por actos del responsable que puedan ser contrarios a lo dispuesto por la presente ley y demás normativa aplicable, o en su caso, por cualquier persona cuando tenga conocimiento de presuntos incumplimientos a las obligaciones previstas en la presente ley y demás disposiciones que resulten aplicables en la materia.

De una interpretación literal de las fracciones anteriormente citadas, se podría considerar que cualquier violación a las disposiciones de esta ley general —o demás disposiciones que resulten aplicables en la materia— podrían ser tema del procedimiento de verificación. Sin embargo, el tercer párrafo del artículo 147 establece una excepción de procedencia, la cual consiste, precisamente, en la exclusión de aquellos supuestos en los que resultan procedentes los recursos de revisión o inconformidad que pueden interponerse ante el INAI o los organismos garantes, dependiendo del caso concreto.

Por lo que se refiere al recurso de revisión, el artículo 104 de la LGPDPPSO establece de manera taxativa los supuestos en el que procede. Los cuales están condicionados —por el artículo 103 de este mismo ordenamiento— a que el titular de los datos personales (o su representante) haya ejercido previamente una solicitud para ejercer sus derechos ARCO. Por otro lado, el artículo 117 establece que el recurso de inconformidad procede únicamente en contra de aquellas resoluciones del recurso de revisión que hayan sido emitidas por un organismo garante. Es decir, la procedencia del recurso de revisión se encuentra condicionada a la existencia previa de una solicitud de ejercicio de derechos ARCO, mientras que el recurso de inconformidad se trata de

una segunda instancia del recurso de revisión cuando éste haya sido tramitado ante un organismo garante.

En consecuencia, si la procedencia de la verificación es excluyente de aquellos supuestos en los que proceden los recursos de revisión o de inconformidad, entonces, el procedimiento de verificación a que se refiere el presente capítulo será procedente únicamente en aquellos supuestos en los que la denuncia de posibles violaciones no se encuentre vinculada de manera directa con el ejercicio de los derechos ARCO.[307]

Cabe decir que, conforme al artículo 148 de la LGPDPPSO, no podrán exigirse más requisitos para la presentación de una denuncia que los ahí estipulados.

**2. Investigaciones previas.** De conformidad con lo establecido en el último párrafo del artículo 147 de la LGPDPPSO, el INAI o los organismos garantes podrán realizar investigaciones previas con la finalidad de obtener los elementos necesarios para fundar y motivar el acuerdo por el cual se inicie, formalmente, el procedimiento de verificación.

El análisis de esta facultad —la realización de investigaciones previas que posteriormente permitan fundar y motivar el inicio del procedimiento de verificación— resulta de suma importancia. Debe quedar claro que la facultad de iniciar investigaciones previas y la facultad de llevar a cabo el procedimiento de verificación se ejercen en dos momentos distintos y tienen objetivos e implicaciones distintas, por lo que es preciso exponer un análisis de ambas facultades y la manera en la que se relacionan una con la otra con la finalidad de dilucidar sus diferencias y las funciones con las que cumple cada una.

Podría interpretarse que la facultad del INAI y los organismos garantes de iniciar investigaciones previas coloca al responsable del tratamiento de datos personales y a los titulares de dichos datos en un terrible estado de incertidumbre jurídica. Lo anterior se debe a que pareciera que este precepto normativo otorga a las instituciones anteriormente mencionadas la facultad de intervenir la esfera jurídica del responsable y, por ende, de los titulares, sin la necesidad de fundar y motivar dicho acto de autoridad, lo que implicaría una violación directa de la CPEUM. Sin embargo, creemos que el otorgamiento y ejercicio de esta facultad, por parte del INAI o los organismos garantes, tiene por objeto la salvaguarda y protección de los derechos del responsable y los titulares, no así la vulneración de los mismos.

[307] Un supuesto diferente es el que contemplan los artículos 161 y 162 del "Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público", publicado en el *Diario Oficial de la Federación* el 26 de enero de 2018, mismos que establecen el procedimiento de verificación "del cumplimiento de las resoluciones de los recursos de revisión", de conformidad con el cual el Instituto deberá verificar de oficio el cumplimiento de dichas resoluciones y dar vista al titular para que éste manifieste lo que a su derecho convenga y, en su caso, que el cumplimiento no corresponde a lo ordenado por el Instituto.

De conformidad con lo establecido en el primer párrafo del artículo 147 de esta ley general, el procedimiento de verificación podrá iniciarse de oficio cuando el INAI o los organismos garantes "cuenten con indicios que hagan presumir fundada y motivada la existencia de violaciones a las leyes correspondientes". A su vez, el artículo 149 establece que "la verificación debe iniciarse mediante una orden escrita que funde y motive la procedencia de la actuación de la autoridad correspondiente". De esta manera, para que pueda iniciarse un procedimiento de verificación es necesario que las autoridades funden y motiven la procedencia de su actuación. Esto es, deben existir indicios de los que se desprenda la posible violación, por parte del responsable del tratamiento de datos personales, de alguna de las disposiciones contenidas en esta ley general o demás ordenamientos aplicables a la materia. Sin embargo, ¿cómo pueden las autoridades obtener o averiguar cuestiones relacionadas con esos indicios? ¿Cuál es el parámetro para determinar que existen indicios de posibles violaciones? ¿Quién debe realizar esas determinaciones? ¿Cuáles son sus implicaciones?

De conformidad con ciertos criterios aislados, un indicio es "[…] una circunstancia cierta de la que se puede sacar, por inducción lógica, una conclusión acerca de la existencia (o inexistencia) de un hecho a probar […]".[308] Puesto que los indicios deben ser circunstancias ciertas, es necesario que exista algún medio de convicción o de prueba con base en el cual pueda sustentarse la posibilidad de que el responsable del tratamiento de datos personales violó las disposiciones de esta ley general u otras disposiciones relacionadas con la materia.

Por lo tanto, el objeto del ejercicio de las facultades de investigación previa que tienen las autoridades anteriormente mencionadas es que puedan realizar acciones encaminadas a la obtención de los medios de prueba o de convicción con base en los cuales pueda determinarse si existen indicios de violaciones a las disposiciones de la ley. Es decir, con base en la información obtenida durante el ejercicio de sus facultades de investigación previa, el INAI o el organismo garante, según corresponda, serán los encargados de calificar si una circunstancia puede o no considerarse un indicio de posibles violaciones a la ley por parte del responsable. En caso de decidir que las circunstancias pueden calificarse como un indicio, la autoridad deberá fundar y motivar dicha decisión. Posteriormente, esa fundamentación y motivación se tomará en cuenta para dar inicio, formalmente, al procedimiento de verificación, donde se analizará si efectivamente el responsable del tratamiento de datos violó las disposiciones de esta ley general y demás disposiciones aplicables. De esta manera, el ejercicio de las facultades de investigación previa por parte de las autoridades y las consideraciones de que existen indicios de posibles violaciones a las

[308] Tribunales Colegiados de Circuito. (julio 1994). Tesis aislada, Octava Época, *Semanario Judicial de la Federación y su Gaceta*. Tomo XIV, p. 621.

disposiciones de esta ley general no prejuzgan sobre la responsabilidad de la persona moral o física encargada del tratamiento de los datos personales, sino únicamente sobre la necesidad de iniciar un procedimiento de verificación.[309]

La obligación del INAI o los organismos garantes de fundamentar y motivar los actos de autoridad que ejercen frente a los sujetos obligados, que en muchas ocasiones también son instituciones gubernamentales, se debe a que el procedimiento de verificación y los actos de autoridad que ellos implican trascienden la esfera jurídica de los titulares de los datos personales que se encuentran sujetos al tratamiento del responsable investigado. De lo contrario, no habría necesidad de fundamentar y motivar los actos de autoridad, pues bastaría que el organismo encargado de realizar la verificación contase con la facultad para hacerlo y se actualicen los supuestos de hecho contenidos en esta ley general.[310]

**3. Instancias de seguridad nacional y seguridad pública.** La LGPDPPSO establece requisitos adicionales para llevar a cabo un procedimiento de verificación ante las instancias de seguridad nacional y seguridad pública. Estos requisitos se encuentran establecidos en el segundo párrafo del artículo 149 de esta ley y consisten en la aprobación de la resolución por parte del pleno del INAI —o de los organismos garantes— con una mayoría calificada,[311] así como "una fundamentación y motivación reforzada de la causa del procedimiento, debiéndose asegurar la información sólo para uso exclusivo de la autoridad y para los fines establecidos en el artículo 150".

El concepto de instancia de seguridad nacional es un concepto que ha sido definido por el legislador. Específicamente, la fracción XXIX-M del artículo 73 de la Constitución concede al Congreso de la Unión la facultad de "expedir leyes en materia de seguridad nacional, estableciendo los requisitos y límites a las investigaciones correspondientes". En este sentido, el legislador determinó en el artículo 6 de la Ley de Seguridad Nacional que deberá entenderse por instancia

[309] No obstante, cabe mencionar que de conformidad con el "Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público", el ejercicio de la facultad de iniciar investigaciones previas supone la posibilidad de expedir "requerimientos de información" dirigidos al responsable, al encargado o a terceros para solicitar información y documentación oportuna; solicitar que éstos se manifiesten respecto de los hechos vertidos en la denuncia, y para que aporten información y documentación que acrediten su dicho (artículo 195). Todo lo cual, en términos de los propios Lineamientos, tiene por objeto fundar y motivar, en su caso, el acuerdo de inicio del procedimiento de verificación (artículo 189).

[310] FUNDAMENTACIÓN Y MOTIVACIÓN. SU CUMPLIMIENTO CUANDO SE TRATE DE ACTOS QUE NO TRASCIENDAN, DE MANERA INMEDIATA, LA ESFERA JURÍDICA DE LOS PARTICULARES. Suprema Corte de Justicia de la Nación. (abril 2000). Tesis jurisprudencial P./J. 50/2000, Novena Época, *Semanario Judicial de la Federación y su Gaceta*. Tomo XI, p. 813.

[311] De conformidad con el artículo 202 del "Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público", publicado en el *Diario Oficial de la Federación* el 26 de enero de 2018, la mayoría calificada del Pleno del INAI hace referencia al voto a favor de por lo menos cinco comisionados.

de seguridad nacional aquellas "instituciones y autoridades que en función de sus atribuciones participen directa o indirectamente en la Seguridad Nacional". De conformidad con el título segundo de esta misma ley, las instancias de seguridad nacional son el Consejo de Seguridad Nacional y el Centro de Investigación y Seguridad Nacional. Dicho lo anterior, es claro que cuando se lleve a cabo un procedimiento de verificación ante el Consejo de Seguridad Nacional o el Centro de Investigación y Seguridad Nacional, será necesario que el INAI: (1) apruebe la resolución que se derive de este procedimiento por una mayoría calificada, (2) funde y motive de manera reforzada el procedimiento y (3) "debiéndose asegurar la información sólo para uso exclusivo de la autoridad y para los fines establecidos en el artículo 150". Las mismas salvaguardas tendrán que adoptarse para el caso de las instancias de seguridad pública tanto por el INAI como por los organismos garantes de las entidades federativas, según corresponda.

La Suprema Corte de Justicia de la Nación ha distinguido en jurisprudencia el concepto de fundamentación y motivación reforzada de la ordinaria. Fundar y motivar de manera ordinaria se ha entendido como la obligación de las autoridades de señalar en sus actos los fundamentos de derecho aplicables al caso concreto, así como las razones de hecho y de derecho que sustenten un acto de autoridad. No obstante, cuando dicho acto pudiera conllevar a la violación de un derecho fundamental o un bien relevante desde el punto de vista constitucional —como la seguridad nacional—, el ejercicio de fundar y motivar deberá realizarse con un mayor grado de complejidad. En este sentido, en el caso de que sea necesaria una fundamentación y motivación reforzada la autoridad deberá ponderar la necesidad de sus actos frente a los intereses constitucionales que estén involucrados en el caso concreto.[312]

**4. Sustanciación del procedimiento.** Si bien la LGPDPPSO contiene un desarrollo escaso sobre la sustanciación del procedimiento de verificación, el Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público, establece que la misma constará tanto de los requerimientos de información, en cuya atención podrán presentarse las pruebas pertinentes, como de las visitas de verificación (artículo 204).

En ningún caso, el responsable del tratamiento de los datos personales podrá negar el acceso a la documentación solicitada, a sus bases de datos personales o al tratamiento de los mismos, ni podrá invocar la reserva o confidencialidad de la información.

El procedimiento de verificación tendrá una duración máxima de cincuenta días hábiles a partir de la notificación del acuerdo de inicio del

[312] MOTIVACIÓN LEGISLATIVA. CLASES, CONCEPTO Y CARACTERÍSTICAS. Suprema Corte de Justicia de la Nación. (diciembre 2009). Tesis jurisprudencial P./J. 120/2009, Novena Época, *Semanario Judicial de la Federación y su Gaceta.* Tomo XXX, p. 1255.

propio procedimiento. De tal forma que, en el cómputo de este plazo, no se considerará el tiempo transcurrido durante la etapa de la investigación previa.

**5. Medidas cautelares.** El artículo 149 de la LGPDPPSO establece la posibilidad para que el INAI o los organismos garantes, según corresponda, ordenen medidas cautelares, "si del desahogo de la verificación advierten un daño inminente o irreparable en materia de protección de datos personales, siempre y cuando no impidan el cumplimiento de las funciones ni el aseguramiento de bases de datos de los sujetos obligados". Se trata, pues, de la adopción de medidas que pretenden garantizar la eficacia de la resolución del procedimiento de verificación.

En términos de nuestros tribunales de justicia, transpolables al caso que nos ocupa, las medidas cautelares "son mecanismos autorizados por la ley para garantizar todo derecho con probabilidad de insatisfacción, mediante la salvaguarda de una situación de hecho, el apartamiento de bienes, cosas o personas para garantizar la eventual realización de la sentencia, o la anticipación de ciertos efectos provisiones de la sentencia de mérito, a fin de evitar la afectación que podría causar la dilación en la resolución de la cuestión sustancial controvertida o la inutilidad del proceso mismo".[313] Todo lo cual se manifiesta a través de la exigencia legal de que exista "daño inminente o irreparable" para su procedencia, así como respecto de su carácter estrictamente temporal con finalidades correctivas (artículo 149 de la LGPDPPSO).

Al respecto, el Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público establece los diversos tipos de medidas cautelares que puede ordenar el Instituto: (1) el cese inmediato del tratamiento, de los actos o las actividades que estén ocasionando o puedan ocasionar un daño; (2) la realización de actos o acciones cuya omisión hayan causado o puedan causar un daño; (3) el bloqueo de los datos personales en posesión del responsable y (4) cualquier otra medida, de acción u omisión que el Instituto considere pertinente dirigida a proteger el derecho a la protección de datos personales. Cualquiera de estos tipos de medida cautelar sólo será procedente ante la posibilidad de que se produzca un daño inminente o irreparable.

**6. Cumplimiento de las resoluciones del procedimiento de verificación.** El artículo 150 de esta ley general establece que el procedimiento de verificación "concluirá con la resolución que emita el Instituto o los organismos garantes,

[313] MEDIDAS CAUTELARES. CONCEPTO, PRESUPUESTOS, MODALIDADES, EXTENSIÓN, COMPLEJIDAD Y AGILIDAD PROCESAL Tribunales Colegiados de Circuito. (agosto 2016).Tesis I.4o.C.4 K (10a.), Décima Época, *Semanario Judicial de la Federación y su Gaceta*, Libro 33, Tomo IV, p. 2653.

en la cual, se establecerán las medidas que deberá adoptar el responsable en el plazo que la misma determine".

Sin duda, una cuestión práctica que puede resultar sumamente compleja es cómo la autoridad que emite una resolución, en este caso el INAI o los organismos garantes, puede comprobar que la misma se cumpla. Al respecto, el Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público establece la rendición de informe de cumplimiento y un procedimiento de verificación del cumplimiento (artículos 216 y 217, respectivamente).

**7. Auditorías voluntarias.** Finalmente, el artículo 151 de la LGPDPPSO establece la posibilidad de que los responsables del tratamiento de datos personales se sometan, voluntariamente, a la realización de auditorías por parte del INAI o de los organismos garantes, a fin de "verificar la adaptación, adecuación y eficacia de los controles, medidas y mecanismos implementados para el cumplimiento de las disposiciones previstas en la presente Ley y demás normativa que resulte aplicable".

Si bien estas auditorías voluntarias no son parte del proceso de verificación, por lo que su ubicación en el presente capítulo puede inducir a la confusión, su objetivo es similar en el sentido de salvaguardar el cumplimiento de los principios y obligaciones del derecho a la protección de datos personales previstos por esta ley y las disposiciones jurídicas que de ella emanan.

## IV. Conclusiones

El procedimiento de verificación es el mecanismo *ad hoc* para que los órganos garantes del derecho a la protección de datos personales puedan investigar, vigilar y comprobar el cumplimiento efectivo de los principios y obligaciones que este derecho humano supone por parte de los sujetos obligados. De igual forma se constituye en una vía para que el Estado cumpla con su obligación de proteger y garantizar los derechos humanos reconocidos en nuestro orden constitucional, de conformidad con el artículo 1º de la CPEUM.

## Referencias

DOF. (2010). Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación*.

DOF. (2011). Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación*.

DOF. (2017). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, *Diario Oficial de la Federación*.

Fix-Zamudio, H. (1978). La función constitucional del Ministerio Público, *Anuario Jurídico*, vol. V, Instituto de Investigaciones Jurídicas de la UNAM.

Instituto Federal de Acceso a la Información Pública (IFAI). (septiembre 2005). Lineamientos de Protección de Datos Personales, *Diario Oficial de la Federación*.

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (enero 2018). Acuerdo mediante el cual se aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público, *Diario Oficial de la Federación*.

Salazar, P. (Coord.). (2014). *La reforma constitucional sobre derechos humanos. Una guía conceptual*. México: Instituto Belisario Domínguez, Senado de la República.

Suprema Corte de Justicia de la Nación. (2000). Tesis jurisprudencial P./J. 50/2000, Novena Época, *Semanario Judicial de la Federación y su Gaceta*. Tomo XI, p. 813.

Suprema Corte de Justicia de la Nación. (2009). Tesis jurisprudencial P./J. 120/2009, Novena Época, *Semanario Judicial de la Federación y su Gaceta*. Tomo XXX, p. 1255.

Tribunales Colegiados de Circuito. (1994). Tesis aislada, Octava Época, *Semanario Judicial de la Federación y su Gaceta*. Tomo XIV, p. 621.

Tribunales Colegiados de Circuito. (2016). Tesis I.4o.C.4 K (10a.), Décima Época, *Semanario Judicial de la Federación y su Gaceta*, Libro 33. Tomo IV, p. 2653.

# TÍTULO DÉCIMO PRIMERO
# MEDIDAS DE APREMIO Y RESPONSABILIDADES

# CAPÍTULO I
# DE LAS MEDIDAS DE APREMIO

***Artículo 152.*** *Para el cumplimiento de las resoluciones emitidas por el Instituto o los Organismos garantes, según corresponda, éstos organismos y el responsable, en su caso, deberán observar lo dispuesto en el Capítulo VI del Título Octavo de la Ley General de Transparencia y Acceso a la Información Pública.*

***Artículo 153.*** *El Instituto y los Organismos garantes podrán imponer las siguientes medidas de apremio para asegurar el cumplimiento de sus determinaciones:*

*I. La amonestación pública, o*

*II. La multa, equivalente a la cantidad de ciento cincuenta hasta mil quinientas veces el valor diario de la Unidad de Medida y Actualización.*

*El incumplimiento de los sujetos obligados será difundido en los portales de obligaciones de transparencia del Instituto y los Organismos garantes y considerados en las evaluaciones que realicen éstos.*

*En caso de que el incumplimiento de las determinaciones del Instituto y los Organismos garantes implique la presunta comisión de un delito o una de las conductas señaladas en el artículo 163 de la presente Ley, deberán denunciar los hechos ante la autoridad competente. Las medidas de apremio de carácter económico no podrán ser cubiertas con recursos públicos.*

***Artículo 154.*** *Si a pesar de la ejecución de las medidas de apremio previstas en el artículo anterior no se cumpliere con la resolución, se requerirá el cumplimiento al superior jerárquico para que en el plazo de cinco días lo obligue a cumplir sin demora.*

*De persistir el incumplimiento, se aplicarán sobre aquéllas medidas de apremio establecidas en el artículo anterior. Transcurrido el plazo, sin que se*

*haya dado cumplimiento, se dará vista la autoridad competente en materia de responsabilidades.*

***Artículo 155.*** *Las medidas de apremio a que se refiere el presente Capítulo, deberán ser aplicadas por el Instituto y los Organismos garantes, por sí mismos o con el apoyo de la autoridad competente, de conformidad con los procedimientos que establezcan las leyes respectivas.*

***Artículo 156.*** *Las multas que fijen el Instituto y los Organismos garantes se harán efectivas por el Servicio de Administración Tributaria o las Secretarías de Finanzas de las Entidades Federativas, según corresponda, a través de los procedimientos que las leyes establezcan.*

***Artículo 157.*** *Para calificar las medidas de apremio establecidas en el presente Capítulo, el Instituto y los Organismos garantes deberán considerar:*

*I. La gravedad de la falta del responsable, determinada por elementos tales como el daño causado; los indicios de intencionalidad; la duración del incumplimiento de las determinaciones del Instituto o los Organismos garantes y la afectación al ejercicio de sus atribuciones;*

*II. La condición económica del infractor, y*

*III. La reincidencia.*

*El Instituto y los Organismos garantes establecerán mediante lineamientos de carácter general, las atribuciones de las áreas encargadas de calificar la gravedad de la falta de observancia a sus determinaciones y de la notificación y ejecución de las medidas de apremio que apliquen e implementen, conforme a los elementos desarrollados en este Capítulo.*

***Artículo 158.*** *En caso de reincidencia, el Instituto o los Organismos garantes podrán imponer una multa equivalente hasta el doble de la que se hubiera determinado por el Instituto o los Organismos garantes.*

*Se considerará reincidente al que habiendo incurrido en una infracción que haya sido sancionada, cometa otra del mismo tipo o naturaleza.*

***Artículo 159.*** *Las medidas de apremio deberán aplicarse e implementarse en un plazo máximo de quince días, contados a partir de que sea notificada la medida de apremio al infractor.*

***Artículo 160.*** *La amonestación pública será impuesta por el Instituto o los organismos garantes y será ejecutada por el superior jerárquico inmediato del infractor con el que se relacione.*

***Artículo 161.*** *El Instituto o los Organismos garantes podrán requerir al infractor la información necesaria para determinar su condición económica, apercibido de que en caso de no proporcionar la misma, las multas se cuantificarán con base a los elementos que se tengan a disposición, entendidos como los que se encuentren en los registros públicos, los que contengan medios de información o sus propias páginas de Internet y, en general, cualquiera que evidencie su condición, quedando facultado el Instituto o los Organismos garantes para requerir aquella documentación que se considere indispensable para tal efecto a las autoridades competentes.*

***Artículo 162.*** *En contra de la imposición de medidas de apremio, procede el recurso correspondiente ante el Poder Judicial de la Federación, o en su caso ante el Poder Judicial correspondiente en las Entidades Federativas.*

## COMENTARIO

**Olivia Andrea Mendoza Enríquez**

### I. Antecedentes

Para comenzar el análisis de este apartado es necesario destacar lo novedoso de la aparición de las medidas de apremio en materia de datos personales. Si bien el artículo 6º constitucional, apartado A, fracción VIII, párrafo sexto reconoce que la ley establecerá las medidas de apremio que podrá imponer el organismo garante para asegurar el cumplimiento de sus decisiones, estas medidas se desarrollan en esta ley específica.

En este sentido, si bien es cierto que la LFTAIPG emitida en 2002 hacía referencia a las responsabilidades y sanciones a los servidores públicos por incumplimiento a las disposiciones de dicha ley, sólo se estableció para determinar la responsabilidad administrativa en lo general. Dentro de sus causales destacaban algunas relacionadas a la protección de datos personales, como las referidas a usar, sustraer, destruir, ocultar, inutilizar, divulgar o alterar total o parcialmente y de manera indebida información que se encontrara bajo su custodia, o a la cual tuvieran acceso o conocimiento con motivo de su empleo, cargo o comisión y la de entregar información considerada como confidencial conforme a lo dispuesto por dicha ley.[314]

Es importante destacar que la responsabilidad a que se refería este artículo o cualquiera otra derivada del incumplimiento de las obligaciones establecidas en dicha ley sería sancionada en los términos de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos (ahora abrogada) y que al menos la

[314] Artículo 63, fracciones I y V de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (abrogada).

entrega de información considerada como confidencial (datos personales) o la reincidencia en las conductas causales de una sanción administrativa, serían consideradas como graves para efectos de su sanción administrativa.

## II. Relevancia temática y de contexto

La inclusión de medidas de apremio en la LGPDPPSO es de suma trascendencia al preverse mecanismos para lograr la ejecución de lo determinado por el Instituto o los organismos garantes, en el ejercicio de una actividad jurisdiccional, es decir, es un mecanismo de efectividad para el total cumplimiento de las resoluciones emitidas por el Pleno del Instituto.

Esto ha permitido que la implementación y cumplimiento de la ley sea tomada como una tarea prioritaria por parte de los sujetos obligados.

## III. Análisis del contenido

El artículo 152 de la LGPDPPSO establece que para el cumplimiento de las resoluciones emitidas por el INAI o los organismos garantes, según corresponda, estos organismos y el responsable, en su caso, deberán observar lo dispuesto en el Capítulo VI del Título Octavo de la LGTAIP, referente a los procedimientos de impugnación en materia de acceso a la información pública, específicamente lo referente al cumplimiento de las resoluciones emitidas por los organismos garantes.

En este sentido, la LGTAIP de 2015, en su artículo 196, establece que los sujetos obligados, a través de la Unidad de Transparencia, darán estricto cumplimiento a las resoluciones de los organismos garantes y deberán informar a éstos sobre su cumplimiento.

También prevé que, excepcionalmente y considerando las circunstancias especiales del caso, los sujetos obligados podrán solicitar a los organismos garantes, de manera fundada y motivada, una ampliación del plazo para el cumplimiento de la resolución. Esta solicitud deberá presentarse, a más tardar, dentro de los primeros tres días del plazo otorgado para el cumplimiento, a efecto de que los organismos garantes resuelvan sobre la procedencia de la misma dentro de los cinco días siguientes.

En el mismo sentido, el artículo 197 de la LGTAIP señala que transcurrido el plazo otorgado para el cumplimiento, el sujeto obligado deberá informar al organismo garante sobre el cumplimento de la resolución.

Por su parte, el organismo garante verificará de oficio la calidad de la información y, a más tardar al día siguiente de recibir el informe, dará vista al recurrente para que, dentro de los cinco días siguientes, manifieste lo que a su derecho convenga. Si dentro del plazo señalado el recurrente manifiesta que el cumplimiento no corresponde a lo ordenado por el organismo garante, deberá expresar las causas específicas por las cuales así lo considera.

El artículo 198 de la LGTAIP prevé que el organismo garante deberá pronunciarse, en un plazo no mayor a cinco días, sobre todas las causas que el recurrente manifieste, así como del resultado de la verificación realizada. Si el organismo garante considera que se dio cumplimiento a la resolución, emitirá un acuerdo de cumplimiento y se ordenará el archivo del expediente. En caso contrario, el organismo garante, deberá:

**I.** Emitir un acuerdo de incumplimiento.
**II.** Notificar al superior jerárquico del responsable de dar cumplimiento, para el efecto de que, en un plazo no mayor a cinco días, se dé cumplimiento a la resolución.
**III.** Determinar las medidas de apremio o sanciones, según corresponda, que deberán imponerse o las acciones procedentes que deberán aplicarse.

Retomando el análisis del apartado de medidas de apremio de la LGPDPPSO, el artículo 153 establece dos tipos de medidas de apremio que pueden ser impuestas por los organismos garantes: la amonestación pública o la multa equivalente a la cantidad de ciento cincuenta hasta mil quinientas veces el valor diario de la Unidad de Medida y Actualización.

Aunado a esto, el incumplimiento de los sujetos obligados será difundido en los portales de obligaciones de transparencia del Instituto y los organismos garantes para ser considerados en las evaluaciones que realicen.

En caso de que el incumplimiento de las determinaciones del Instituto y los organismos garantes implique la presunta comisión de un delito o una de las conductas señaladas en el artículo 163 de la ley comentada (causales de sanciones) deberán denunciar los hechos ante la autoridad competente.

Un aspecto importante es que las medidas de apremio de carácter económico no podrán ser cubiertas con recursos públicos, sino con los del propio servidor público o persona a quien se le haya acreditado el incumplimiento a las disposiciones de la LGPDPPSO.

El artículo 154 de la LGPDPPSO establece que si a pesar de la ejecución de las medidas de apremio, señaladas en los párrafos anteriores, no se cumpliere

con la resolución, se requerirá el cumplimiento al superior jerárquico para que en el plazo de cinco días lo obligue a cumplir sin demora, y en caso de persistir el incumplimiento, se aplicarán sobre aquellas medidas de apremio establecidas en el artículo anterior. Transcurrido el plazo, sin que se haya dado cumplimiento, se dará vista a la autoridad competente en materia de responsabilidades.

Es importante señalar que la redacción del segundo párrafo del artículo 154 resulta confusa, ya que si bien habla de que una vez que se hayan ejecutado las medidas de apremio y no se cumpliere con la resolución del Instituto o de los organismos garantes, se requerirá el cumplimiento al superior jerárquico para que en el plazo de cinco días se obligue a cumplir sin demora; sin embargo, también establece que de persistir el incumplimiento, se aplicarán sobre aquellas medidas de apremio, dejando en confusión al operador de la ley, ya que no determina a cuáles medidas de apremio y a quién se le aplicarán, en un entendido de encontrarnos frente a un segundo incumplimiento de la resolución emitida.

El artículo 155 señala que las medidas de apremio deberán ser aplicadas por el Instituto y los organismos garantes, por sí mismos o con el apoyo de la autoridad competente, de conformidad con los procedimientos que establezcan las leyes respectivas.

El artículo 156 determina que las multas que fijen el Instituto y los organismos garantes se harán efectivas por el Servicio de Administración Tributaria o las secretarías de Finanzas de las entidades federativas, según corresponda, a través de los procedimientos que las leyes establezcan.

Por otro lado, el artículo 157 establece los criterios que el Instituto o los organismos garantes deben de considerar para calificar las medidas de apremio, los cuales consisten en:

**I.** La gravedad de la falta del responsable, determinada por elementos tales como el daño causado, los indicios de intencionalidad, la duración del incumplimiento de las determinaciones del Instituto o los organismos garantes y la afectación al ejercicio de sus atribuciones.
**II.** La condición económica del infractor
**III.** La reincidencia.

También establece la facultad para que el Instituto y los organismos garantes emitan lineamientos de carácter general, a fin de determinar las atribuciones de las áreas encargadas de calificar la gravedad de la falta de observancia a sus determinaciones y de la notificación y ejecución de las medidas de apremio que apliquen e implementen.

El artículo 158 de la LGPDPPSO, habla del supuesto de servidores públicos reincidentes, en el que el Instituto o los organismos garantes podrán imponer una multa equivalente hasta el doble de la que se hubiera determinado por el Instituto o los organismos garantes. Para tal efecto, se considera reincidente al que, habiendo incurrido en una infracción que haya sido sancionada, cometa otra del mismo tipo o naturaleza.

Por su parte, el artículo 159 de la LGPDPPSO establece que las medidas de apremio deberán aplicarse e implementarse en un plazo máximo de quince días, contados a partir de que sea notificada la medida de apremio al infractor.

Una vez que se ha hablado de las medidas de apremio de carácter económico, el artículo 160 de la LGPDPPSO refiere lo dispuesto a la amonestación pública, la cual será impuesta por el Instituto o los organismos garantes y será ejecutada por el superior jerárquico inmediato del infractor con el que se relacione.

El artículo 161 señala que el Instituto o los organismos garantes podrán requerir al infractor la información necesaria para determinar su condición económica, apercibido de que en caso de no proporcionarla, las multas se cuantificarán con base en los elementos que se tengan a disposición, entendidos como los que se encuentren en los registros públicos, los que contengan medios de información o sus propias páginas de internet y, en general, cualquiera que evidencie su condición, quedando facultado el Instituto o los organismos garantes para requerir aquella documentación que se considere indispensable para tal efecto a las autoridades competentes.

Finalmente, el artículo 162 de la LGPDPPSO habla de los recursos que tienen los servidores públicos en contra de la imposición de medidas de apremio, particularmente el recurso correspondiente ante el Poder Judicial de la Federación, o en su caso, ante el Poder Judicial correspondiente en las entidades federativas.[315]

Es motivo de celebración que una ley en materia de datos personales en posesión de sujetos obligados tenga previstas medidas de apremio que permitan fortalecer el ejercicio de la actividad jurisdiccional tanto del Instituto

[315] En este sentido, es importante señalar que las resoluciones emitidas por el INAI o los organismos garantes son inatacables por parte de los servidores públicos, no así, la imposición de medidas de apremio, que pudieran ser contempladas dentro de dichas resoluciones. Es importante mencionar que la única excepción a lo aquí establecido es el recurso de revisión en materia de seguridad nacional, promovido por el Consejero Jurídico del Ejecutivo ante la Suprema Corte de Justicia de la Nación, a fin de combatir resoluciones dictadas por el órgano garante, siempre que la información relacionada a las mismas, ponga en peligro la seguridad nacional del país. Esto atendiendo a lo dispuesto por el artículo 6º constitucional, letra A, fracción VIII, párrafo séptimo y por los artículos 189, 190, 191, 192 y 193 de la Ley General de Transparencia y Acceso a la Información Pública de mayo de 2015.

como de los organismos garantes.[316] Sin embargo, existen dudas sobre planteamientos vigentes, respecto a si las medidas de apremio de carácter económico deben o no ser cubiertas con recursos públicos.[317]

En este sentido, es importante decir que no podrían afectarse recursos públicos por el incumplimiento que un sujeto obligado en lo particular haya tenido[318] respecto de las disposiciones de ley. En el mismo tenor, se considera idóneo que las medidas de apremio de carácter económico impuestas a los sujetos obligados, una vez que sean ingresadas a la Tesorería de la Federación o su homóloga en las entidades federativas, pudieran ser destinadas a promover la cultura de la protección de datos personales en el país, o en su caso, tuvieran como fin la reparación del daño causado al titular del dato personal derivado del incumplimiento a la normativa en la materia.

Por otro lado, resulta importante la difusión en los portales de obligaciones de transparencia del Instituto y de los organismos garantes, de las medidas de apremio impuestas a los sujetos obligados, derivadas del incumplimiento de la ley en la materia y, sobre todo, la consideración de las mismas en las evaluaciones realizadas por parte del INAI y los organismos garantes a los sujetos obligados, ya que esto fortalece el escrutinio público y la evaluación ciudadana a los sujetos de la ley.

Los mecanismos propuestos por la LGPDPPSO permiten al Instituto y a los organismos garantes dar un seguimiento puntual al cumplimiento de las resoluciones y de la imposición de medidas de apremio. Sin embargo, resulta cuestionable trasladar dichas medidas al superior jerárquico del servidor público en rebeldía, en el plazo de cinco días, ya que en la práctica, podría tratarse de un secretario de Estado, el cual en el tiempo establecido por la ley, se vería imposibilitado a tomar las medidas y acciones necesarias para subsanar el incumplimiento. No obstante, lo anterior es un mecanismo de presión efectivo para el cumplimiento de las medidas de apremio en los plazos claramente señalados por la ley, sin importar el nivel jerárquico del que se trate.

Finalmente, es importante señalar que se retoman disposiciones de la LFTAIPG de 2002, relacionadas a las vías que podrían seguirse, derivado del

[316] En la imposición de medidas de apremio, se deben respetar las garantías de legalidad y seguridad jurídica que establecen los artículos 14 y 16 constitucionales.

[317] Para tal efecto, el Reglamento Europeo de Protección de Datos Personales 2016/679, que será de plena aplicación a partir de mayo de 2018, establece en el artículo 83 respecto de las condiciones generales para la imposición de multas administrativas, particularmente en el numeral 7, que sin perjuicio de los poderes correctivos de las autoridades de control, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro.

[318] Es importante señalar que las medidas de apremio no sólo pueden ser impuestas a servidores públicos, ya que de acuerdo con el artículo 1 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, los partidos políticos son considerados como sujetos obligados y sus integrantes no necesariamente son servidores públicos.

incumplimiento de la ley, por ejemplo, en materia civil, administrativa o penal y que una no agota a la otra.

Se destaca la facultad que tiene el Instituto o los organismos garantes para denunciar los hechos contrarios a la ley ante autoridades como los ministerios públicos, el Instituto Nacional Electoral u organismos locales en la materia, los poderes legislativos o ante la Secretaría de la Función Pública y los órganos de control interno.

## IV. Conclusiones

Resulta relevante reforzar el cumplimiento de las disposiciones en materia de protección de datos personales en posesión de sujetos obligados con medidas de apremio como las señaladas en párrafos anteriores. Sin embargo, se enfatiza que existe una alta expectativa en la ley para la efectiva protección de los datos personales, cuando se ha demostrado que, si las disposiciones normativas no van acompañadas, por ejemplo, de acciones concretas que promuevan la cultura de la protección de datos personales, y que con ello, se permita romper el paradigma del tratamiento de la información en el sector público, poco se podrá hacer para la efectiva tutela de un derecho humano como el que se garantiza en la LGPDPPSO.

## Referencias

DOF. (2014). Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, *Diario Oficial de la Federación*.

DOF. (2015). Ley General de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*.

DOF. (2016). Ley Federal de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*.

DOF. (2017). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, *Diario Oficial de la Federación*.

Parlamento Europeo y del Consejo. (2016). Reglamento 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), *Diario Oficial de la Unión Europea*.

# CAPÍTULO II
# DE LAS SANCIONES

***Artículo 163.*** *Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes:*

*I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO;*

*II. Incumplir los plazos de atención previstos en la presente Ley para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate;*

*III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;*

*IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley;*

*V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos a que refiere el artículo 27 de la presente Ley, según sea el caso, y demás disposiciones que resulten aplicables en la materia;*

*VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. La sanción sólo procederá cuando exista una resolución previa, que haya quedado firme, respecto del criterio de clasificación de los datos personales;*

*VII. Incumplir el deber de confidencialidad establecido en el artículo 42 de la presente Ley;*

*VIII. No establecer las medidas de seguridad en los términos que establecen los artículos 31, 32 y 33 de la presente Ley;*

*IX. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad según los artículos 31, 32 y 33 de la presente Ley;*

*X. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la presente Ley;*

*XI. Obstruir los actos de verificación de la autoridad;*

*XII. Crear bases de datos personales en contravención a lo dispuesto por el artículo 5 de la presente Ley;*

*XIII. No acatar las resoluciones emitidas por el Instituto y los Organismos garantes, y*

*XIV. Omitir la entrega del informe anual y demás informes a que se refiere el artículo 44, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública, o bien, entregar el mismo de manera extemporánea.*

*Las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, y XIV, así como la reincidencia en las conductas previstas en el resto de las fracciones de este artículo, serán consideradas como graves para efectos de su sanción administrativa.*

*En caso de que la presunta infracción hubiere sido cometida por algún integrante de un partido político, la investigación y, en su caso, sanción, corresponderán a la autoridad electoral competente.*

*Las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.*

***Artículo 164.*** *Para las conductas a que se refiere el artículo anterior se dará vista a la autoridad competente para que imponga o ejecute la sanción.*

***Artículo 165.*** *Las responsabilidades que resulten de los procedimientos administrativos correspondientes, derivados de la violación a lo dispuesto por el artículo 163 de esta Ley, son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos.*

*Dichas responsabilidades se determinarán, en forma autónoma, a través de los procedimientos previstos en las leyes aplicables y las sanciones que, en su caso, se impongan por las autoridades competentes, también se ejecutarán de manera independiente.*

*Para tales efectos, el Instituto o los organismos garantes podrán denunciar ante las autoridades competentes cualquier acto u omisión violatoria de esta Ley y aportar las pruebas que consideren pertinentes, en los términos de las leyes aplicables.*

***Artículo 166.*** *Ante incumplimientos por parte de los partidos políticos, el Instituto u organismo garante competente, dará vista, según corresponda, al Instituto Nacional Electoral o a los organismos públicos locales electorales de las Entidades Federativas competentes, para que resuelvan lo conducente, sin perjuicio de las sanciones establecidas para los partidos políticos en las leyes aplicables.*

*En el caso de probables infracciones relacionadas con fideicomisos o fondos públicos, el Instituto u organismo garante competente deberá dar vista al órgano interno de control del sujeto obligado relacionado con éstos, cuando sean servidores públicos, con el fin de que instrumenten los procedimientos administrativos a que haya lugar.*

***Artículo 167.*** *En aquellos casos en que el presunto infractor tenga la calidad de servidor público, el Instituto o el organismo garante, deberá remitir a la autoridad competente, junto con la denuncia correspondiente, un Expediente en que se contengan todos los elementos que sustenten la presunta responsabilidad administrativa.*

*La autoridad que conozca del asunto, deberá informar de la conclusión del procedimiento y, en su caso, de la ejecución de la sanción al Instituto o al organismo garante, según corresponda.*

*A efecto de sustanciar el procedimiento citado en este artículo, el Instituto, o el organismo garante que corresponda, deberá elaborar una denuncia dirigida a la contraloría, órgano interno de control o equivalente, con la descripción precisa de los actos u omisiones que, a su consideración, repercuten en la adecuada aplicación de la presente Ley y que pudieran constituir una posible responsabilidad.*

*Asimismo, deberá elaborar un expediente que contenga todos aquellos elementos de prueba que considere pertinentes para sustentar la existencia de la posible responsabilidad. Para tal efecto, se deberá acreditar el nexo causal existente entre los hechos controvertidos y las pruebas presentadas.*

*La denuncia y el Expediente deberán remitirse a la contraloría, órgano interno de control o equivalente dentro de los quince días siguientes a partir de que el Instituto o el organismo garante correspondiente tenga conocimiento de los hechos.*

***Artículo 168.*** *En caso de que el incumplimiento de las determinaciones de los Organismos garantes implique la presunta comisión de un delito, el organismo garante respectivo deberá denunciar los hechos ante la autoridad competente.*

# COMENTARIO

**Olivia Andrea Mendoza Enríquez**

## I. Antecedentes

La LFTAIPG de 2002 consideraba causales de responsabilidades administrativas y sanciones relacionadas (algunas) al incumplimiento de las obligaciones en materia de protección de datos personales, dentro de las cuales se encontraban las de usar, sustraer, destruir, ocultar, inutilizar, divulgar o alterar, de manera indebida, información —incluidos datos personales— que se encontraran en custodia de un servidor público, o a la cual tuviera acceso o conocimiento con motivo de su empleo, cargo o comisión y la de entregar información considerada como confidencial, la cual podría estar relacionada a datos personales.[319]

En el mismo ordenamiento establecía que las responsabilidades que fueran determinadas por autoridad competente, derivadas del incumplimiento de las obligaciones en materia de protección de datos personales, serían sancionadas en los términos de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.[320]

Aunado a lo anterior, se establecía que la reincidencia en las conductas descritas en líneas previas, serían consideradas como graves para efectos de su sanción administrativa.

Es importante decir que al igual que en la actual LGPDPPSO, la LFTAIPG también dejaba reservadas las vías civiles o penales, a fin de determinar diversas acciones legales procedentes como consecuencia del incumplimiento de obligaciones en la materia.

El artículo 37 de la LFTAIPG también dotaba de facultades al entonces Instituto Federal de Acceso a la Información Pública para vigilar y, en caso de incumplimiento, hacer las recomendaciones a las dependencias y entidades para que se diera cumplimiento a las obligaciones en materia de transparencia, aunque no se reconocía, de manera expresa, dicha facultad dirigida al cumplimiento de las obligaciones en materia de protección de datos personales.

No obstante lo anterior, el Instituto tenía facultades para hacer del conocimiento del órgano interno de control de cada dependencia y entidad las presuntas infracciones a las disposiciones de la LFTAIPG y su Reglamento.

[319] Artículo 63 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental de 2002.

[320] Esta legislación fue abrogada en términos del transitorio tercero de la Ley General de Responsabilidades Administrativas publicada el 18 de julio de 2016.

En consonancia, la LFTAIPG establecía que el recurso de revisión sustanciado por el IFAI procedía en lugar del recurso de revisión establecido en el artículo 83 de la Ley Federal de Procedimiento Administrativo. En este sentido, cuando el Instituto determinara durante la sustanciación del procedimiento que algún servidor público pudo haber incurrido en responsabilidad, debería hacerlo del conocimiento del órgano interno de control de la dependencia o entidad responsable para que ésta iniciara, en su caso, el procedimiento de responsabilidad que correspondiera.

## II. Relevancia temática y contexto

Es importante destacar que, por primera vez en México, existe una LGPDPPSO que permite tener un régimen claro respecto del tratamiento de los datos personales, especialmente en el sector púbico.[321]

La relevancia de esta legislación no sólo refiere a la adopción de estándares internacionales para el tratamiento de datos personales, ejercicio de los derechos ARCO y los recursos de los titulares de dichos datos, para la efectiva garantía del derecho, sino también a un conjunto de facultades y atribuciones que se otorgan a distintas autoridades a fin de poder establecer medidas de apremio y sanciones derivadas del incumplimiento a la ley.

La imposición de estas sanciones es de carácter administrativo y derivarán del incumplimiento de las obligaciones en materia de protección de datos personales.

Esto resulta trascendental para la efectiva protección de la información personal, ya que el incumplimiento a las disposiciones en la materia podría traer como consecuencia la imposición de sanciones económicas, que deberán ser pagadas con los recursos propios del infractor.

## III. Análisis del contenido

El artículo 163 de la LGPDPPSO establece como causas de sanción por incumplimiento de las obligaciones en materia de protección de datos personales, las siguientes:

I. Actuar con negligencia, dolo o mala fe durante la sustanciación de las solicitudes para el ejercicio de los derechos ARCO. En este sentido, es importante decir que, al no definir elementos como la negligencia o mala fe, se establecen como elementos subjetivos del supuesto sancionable, por lo que podría afectarse el principio de estricta legalidad, e incluso podría ser un obstáculo en la determinación de responsabilidades.

[321] Los datos personales normados por esta legislación, corresponden en su mayoría a aquellos en posesión del sector público; sin embargo, también regula los datos personales en posesión de partidos políticos, los cuales no se encuentran necesariamente en un régimen público.

II. Incumplir los plazos de atención previstos en la LGPDPPSO para responder las solicitudes para el ejercicio de los derechos ARCO o para hacer efectivo el derecho de que se trate. Se observa que a pesar de haberse armonizado los plazos de atención del ejercicio de derechos, tanto de acceso a la información como de protección de datos personales, y que éstos son los mismos para todos los órdenes de gobierno y sujetos obligados de la ley, existe la necesidad de sensibilizar a los operadores de la legislación en la materia, en términos de los supuestos en los que los titulares de datos personales solicitan acceso a los mismos, ya que tratándose de solicitudes de acceso a datos personales contenidos en expedientes clínicos, resulta primordial atender dicha solicitud, sin necesariamente agotar los plazos máximos previstos en la legislación, ya que podría significar la vida o muerte de una persona; es decir, atendiendo a los instrumentos de interpretación de los derechos humanos, no sólo resulta deseable, sino obligatorio dar atención oportuna a las solicitudes de ejercicio de derechos como el de acceso a datos personales.

III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión.

IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la LGPDPPSO. En este sentido, es importante destacar que, tratándose de datos personales de niños, niñas y adolescentes (a pesar de no ser un principio establecido en la ley analizada) se deberá observar, de manera transversal, el principio del interés superior del menor para determinar la protección más amplia a dicha información.

V. No contar con el aviso de privacidad, o bien, omitir en el mismo alguno de los elementos indispensables descritos en la LGPDPPSO.

VI. Clasificar como confidencial, con dolo o negligencia, datos personales sin que se cumplan las características señaladas en las leyes que resulten aplicables. En este caso, la sanción sólo procederá cuando exista una resolución previa que haya quedado firme, respecto del criterio de clasificación de los datos personales.

VII. Incumplir el deber de confidencialidad. Éste puede establecerse a través de cláusulas contractuales, y subsistirá aún después de finalizar la vigencia del contrato.

VIII. No establecer las medidas de seguridad necesarias y establecidas en la LGPDPPSO.

IX. En relación con la anterior fracción, presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad.

X. Llevar a cabo la transferencia de datos personales en contravención a lo previsto en la LGPDPPSO.

XI. Obstruir los actos de verificación de la autoridad. Esta fracción aplica tanto para las verificaciones de oficio, como de las que deriven de la denuncia ante el INAI por el presunto incumplimiento a las obligaciones en materia de protección de datos personales. Esta fracción no aplica a las verificaciones voluntarias solicitadas al Instituto por parte de los sujetos obligados.

XII. Crear bases de datos personales en contravención a las disposiciones de la LGPDPPSO.

XIII. No acatar las resoluciones emitidas por el Instituto y los organismos garantes. Para tal efecto se puede dar aviso al superior jerárquico del sujeto obligado del que se trate.

XIV. Omitir, recabar y enviar al organismo garante los datos necesarios para la elaboración del informe anual, o bien, entregar el mismo de manera extemporánea.

También se establece que la reincidencia y las causas de responsabilidad previstas en las fracciones I, II, IV, VI, X, XII, y XIV del artículo 163 de la LGPDPPSO, analizado en este apartado, serán consideradas como graves, a efectos de su sanción administrativa.

En caso de que la presunta infracción sea cometida por algún integrante de un partido político, la investigación y, en su caso, sanción, corresponderán a la autoridad electoral competente. Además, las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

Por otro lado, el artículo 164 de la LGPDPPSO establece que en el caso de acreditarse alguna de las causales de sanción, se dará vista a la autoridad competente para que imponga o ejecute la sanción correspondiente.

Como se ha dicho en líneas previas, la LGPDPPSO deja salvaguardada la posibilidad de acudir a otras instancias, derivado de la vulneración al derecho a la protección de datos personales en posesión de sujetos obligados. En este sentido, el artículo 165 establece que las responsabilidades que resulten de

los procedimientos administrativos correspondientes son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos, y que dichas responsabilidades se determinarán, en forma autónoma, a través de los procedimientos previstos en las leyes aplicables y las sanciones que, en su caso, se impongan por las autoridades competentes y también se ejecutarán de manera independiente.

Para tales efectos, el Instituto o los organismos garantes podrán denunciar ante las autoridades competentes cualquier acto u omisión violatoria de la LGPDPPSO y aportar las pruebas que consideren pertinentes, en los términos de las leyes aplicables.

El artículo 166 de la LGPDPPSO establece una situación específica relacionada a los incumplimientos por parte de los partidos políticos, ante los cuales, el INAI u organismos garantes competentes, darán vista, según corresponda, al Instituto Nacional Electoral o a los organismos públicos locales electorales de las entidades federativas competentes, para que resuelvan lo conducente sin perjuicio de las sanciones establecidas para los partidos políticos en las leyes aplicables. En el caso de probables infracciones relacionadas con fideicomisos o fondos públicos, el Instituto u organismo garante competente deberá dar vista al órgano interno de control del sujeto obligado relacionado con éstos, cuando sean servidores públicos, con el fin de que instrumenten los procedimientos administrativos a que haya lugar.

Por otro lado, el artículo 167 señala que en aquellos casos en que el presunto infractor tenga la calidad de servidor público, el Instituto o el organismo garante, deberá remitir a la autoridad competente, junto con la denuncia correspondiente, un expediente en que se contengan todos los elementos que sustenten la presunta responsabilidad administrativa. La autoridad que conozca del asunto deberá informar de la conclusión del procedimiento y, en su caso, de la ejecución de la sanción al Instituto o al organismo garante, según corresponda.

A efecto de sustanciar el procedimiento citado en este artículo, el Instituto u organismo garante que corresponda deberá elaborar una denuncia dirigida a la contraloría, órgano interno de control o equivalente, con la descripción precisa de los actos u omisiones que, a su consideración, repercuten en la adecuada aplicación de la presente ley y que pudieran constituir una posible responsabilidad. Asimismo, deberá elaborar un expediente que contenga todos aquellos elementos de prueba que considere pertinentes para sustentar la existencia de la posible responsabilidad. Para tal efecto, se deberá acreditar el nexo causal existente entre los hechos controvertidos y las pruebas presentadas. La denuncia y el expediente deberán remitirse a la contraloría, órgano interno de control o equivalente dentro de los quince días siguientes a partir de que el Instituto o el organismo garante correspondiente tengan conocimiento de los hechos.

Para finalizar el análisis del apartado de sanciones, el artículo 168 establece al INAI y los organismos garantes el deber de denunciar hechos ante autoridad competente, cuando deriven del incumplimiento de sus determinaciones e impliquen la presunta comisión de un delito.

Es primordial destacar la importancia de establecer sanciones y, en su caso, medidas de apremio, a fin de poder garantizar la efectividad de las disposiciones en la ley. Sin embargo, no es viable depositar todas las expectativas en el cumplimiento de la efectiva a garantía del derecho a la protección de datos personales solamente con elementos como la imposición de sanciones.

Las causales de imposición de sanciones están claramente definidas, salvo elementos como la negligencia o la mala fe, lo cual podría propiciar argumentos por parte de los sujetos sancionados, respecto a la violación al principio de estricta legalidad, es decir, los sujetos obligados que estimen vulnerado el principio de legalidad podrán ejercer un medio de defensa,[322] idóneo y adecuado para defensa de sus intereses y derechos del orden administrativo.

Por otro lado, es de resaltar que la LGPDPPSO establece corresponsabilidades entre los sujetos obligados (responsables) y encargados de los datos personales. Esto resulta pertinente, sobre todo cuando estamos ante contrataciones a terceros, por ejemplo, de servicios de cómputo en la nube.

Es importante decir que, si bien las resoluciones del INAI o de los organismos garantes son inatacables para los sujetos obligados, la imposición de medidas de apremio y sanciones puede combatirse a través del Juicio de Nulidad ante el Tribunal de Justicia Fiscal y Administrativa. En otras palabras, los sujetos obligados de la LGPDPPSO no pueden recurrir a las resoluciones emitidas por el Instituto o los organismos garantes, pero sí pueden recurrir a las medidas de apremio y/o sanciones impuestas por autoridad competente y derivadas del incumplimiento de las obligaciones en materia de protección de datos personales.

Se advierte de la complejidad de poder hacer efectivas las sanciones relacionadas a la vulneración al derecho de protección de datos personales a los integrantes de los partidos políticos, ya que, si bien las autoridades electorales están facultadas para hacerlo, no se advierte el mismo control para el cumplimiento, como sí lo tendría un servidor público.

[322] Reconocido en el artículo 14 la Constitución Política de los Estados Unidos Mexicanos.

## IV. Conclusiones

Para lograr la efectiva protección de los datos personales, se deberá impulsar la cultura en estos temas, a fin de poder romper paradigmas en el tratamiento de la información de las personas, sobre todo en el sector público y partidos políticos.

Otro aspecto importante, es poder advertir que los recursos económicos que ingresen al Estado mexicano por la imposición de sanciones económicas derivadas del incumplimiento de la LGPDPPSO no tienen una delimitación en su uso, por lo que no se garantiza que se puedan utilizar, por ejemplo, en acciones concretas de sensibilización, capacitación, y en su caso, resarcimiento del daño causado por vulneraciones al derecho de protección de datos personales.

## Referencias

DOF. (1994). Ley Federal de Procedimiento Administrativo, *Diario Oficial de la Federación*.

DOF. (2014). Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia, *Diario Oficial de la Federación*.

DOF. (2015). Ley General de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*.

DOF. (2016). Ley Federal de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*.

DOF. (2016). Ley General de Responsabilidades Administrativas, *Diario Oficial de la Federación*.

DOF. (2017). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, *Diario Oficial de la Federación*.

# TRANSITORIOS

***Primero.*** *La presente Ley entrará en vigor al día siguiente de su publicación en el Diario Oficial de la Federación.*

***Segundo.*** *La Ley Federal de Transparencia y Acceso .a la Información Pública, las demás leyes federales y las leyes vigentes de las Entidades Federativas en materia de protección de datos personales, deberán ajustarse a las disposiciones previstas en esta norma en un plazo de seis meses siguientes contado a partir de la entrada en vigor de la presente Ley.*

*En caso de que el Congreso de la Unión o las Legislaturas de las Entidades Federativas omitan total o parcialmente realizar las adecuaciones legislativas a que haya lugar, en el plazo establecido en el párrafo anterior, resultará aplicable de manera directa la presente Ley, con la posibilidad de seguir aplicando de manera supletoria las leyes preexistentes en todo aquello que no se oponga a la misma, hasta en tanto no se cumpla la condición impuesta en el presente artículo.*

***Tercero.*** *La Cámara de Diputados, las Legislaturas de las Entidades Federativas, en el ámbito de sus respectivas competencias, deberán hacer las previsiones presupuestales necesarias para la operación de la presente Ley y establecer las partidas presupuestales específicas en el Presupuesto de Egresos de la Federación y en los Presupuestos de Egresos de las Entidades Federativas, según corresponda, para el siguiente ejercicio fiscal a su entrada en vigor.*

***Cuarto.*** *Se derogan todas aquellas disposiciones en materia de protección de datos personales, de carácter federal, estatal y municipal, que contravengan lo dispuesto por la presente Ley.*

***Quinto.*** *El Instituto y los Organismos garantes deberán emitir los lineamientos a que se refiere esta Ley y publicarlos en el Diario Oficial de la Federación, o en sus Gacetas o Periódicos Oficiales locales, respectivamente, a más tardar en un año a partir de la entrada en vigor del presente Decreto.*

***Sexto.*** *El Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales deberá emitir el Programa Nacional de Protección de Datos Personales a que se refiere esta Ley y publicarlo en el Diario Oficial de la Federación, a más tardar en un año a partir de la entrada en vigor del presente Decreto, independientemente del ejercicio de otras atribuciones que se desprenden de la Ley General de Transparencia y Acceso a la Información Pública.*

***Séptimo.*** *Los sujetos obligados correspondientes deberán tramitar, expedir o modificar su normatividad interna a más tardar dentro de los dieciocho meses siguientes a la entrada en vigor de esta Ley.*

***Octavo.*** *No se podrán reducir o ampliar en la normatividad de las Entidades Federativas, los procedimientos y plazos vigentes aplicables en la materia, en perjuicio de los titulares de datos personales.*

## COMENTARIO

**María Solange Maqueo**

### I. Antecedentes

Los artículos transitorios constituyen una parte esencial de una adecuada técnica legislativa. Si bien son normas de carácter secundario que, incluso, cuentan con una numeración diferenciada en la ley, al margen de los títulos o capítulos de la misma, se constituyen en verdaderas disposiciones jurídicas de carácter vinculante. Se trata, pues, de normas jurídicas que forman parte del ordenamiento jurídico y, en consecuencia, su aplicación es de observancia obligatoria.[323]

### II. Relevancia temática y contexto

En cuanto a su naturaleza jurídica, el régimen general de los transitorios parte de la idea de considerarlos como “normas de normas”, a fin de establecer las condiciones y el modo en que deberán aplicarse las disposiciones jurídicas que

[323] ARTÍCULOS TRANSITORIOS. FORMAN PARTE DEL ORDENAMIENTO JURÍDICO RESPECTIVO Y SU OBSERVANCIA ES OBLIGATORIA. Segundo Tribunal Colegiado en materia Administrativa del Sexto Circuito. (2001). Tesis VI.2o.A.1K, Novena Época, *Semanario Judicial de la Federación y su Gaceta*. Tomo XIV p. 1086.

regulan propiamente la materia que es objeto del ordenamiento jurídico, a partir de su introducción mediante modificaciones, adiciones o creación legislativa o regulatoria.[324] Se trata, pues, de un "tipo de normas secundarias relativas a la adjudicación, ya que a pesar de que producen un cambio en el orden jurídico, son disposiciones jurídicas cuyo objeto es determinar el modo de aplicación de otras normas. […] Las normas son el objeto respecto del cual se realiza la acción, son un elemento del supuesto, pero no el sujeto a quien se dirige la norma".[325]

De acuerdo con lo anterior, los artículos transitorios son, como su nombre lo indica, disposiciones jurídicas de carácter vinculante que tienen un carácter provisional o temporal, a fin de facilitar el tránsito de un régimen anterior a uno nuevo, introducido precisamente por la modificación, adición, abrogación, derogación o creación normativa.

## III. Análisis del contenido

Si bien el contenido de los artículos transitorios no está predeterminado, de tal manera que el legislador tiene amplias facultades para establecer el régimen o situación especial que considere conveniente para aplicar las disposiciones jurídicas que se derivan de una reformulación legislativa, por lo general, los artículos transitorios comprenden: la entrada en vigor de la ley o decreto, la pérdida de vigencia de la ley o leyes anteriores, relacionadas con la nueva ley, así como las disposiciones provisionales que generan un régimen de transitoriedad[326] (sea como mandatos dirigidos al propio legislador como a los sujetos regulados por la misma y a los órganos o instituciones encargados de su ejecución).

Al respecto, el artículo Primero Transitorio de esta ley general establece que entrará en vigor al día siguiente a su publicación. De esta forma, el citado artículo adopta el llamado *sistema sincrónico* previsto en el artículo 4º del Código Civil Federal, a través del cual el inicio de vigencia de la LGPDPPSO se encuentra especificado por el propio legislador.

No obstante, este plazo previsto para la entrada en vigor de la ley general se distingue de los plazos previstos para su aplicación y el despliegue de su obligatoriedad, mismos que a su vez están diferenciados de acuerdo con los diversos sujetos a quienes se dirige el mandato.

---

[324] Muro, E. (2007). *Algunos Elementos de Técnica Legislativa*. México: Instituto de Investigaciones Jurídicas de la UNAM. [Archivo PDF]. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/5/2149/2.pdf, [fecha de consulta: 8 de mayo 2018].

[325] Huerta, K. (200). Artículos Transitorios y Derogación, *Boletín Mexicano de Derecho Comparado*, núm. 102, septiembre-diciembre. México: Instituto de Investigaciones Jurídicas de la UNAM, pp. 811-840.

[326] López, M. (2000). "Técnica legislativa y proyectos de ley", en Carbonell, Miguel y Pedroza de la Llave, Susana T. (Coords.), *Elementos de Técnica Legislativa.* México: UNAM.[Archivo PDF]. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/1/21/tc.pdf, [fecha de consulta: 8 de mayo 2018].

En el primer supuesto, cabe destacar que por tratarse de una ley general que regula un régimen de facultades concurrentes y, en consecuencia, supone la función legislativa de las entidades federativas para armonizar su propia legislación en la materia, la obligatoriedad de sus disposiciones jurídicas (principios, deberes y procedimientos) está sujeta a un plazo que permita su adopción y ajuste por parte de las legislaturas estatales.[327] Este plazo es de seis meses a partir de la entrada en vigor de la ley, de conformidad con el artículo Segundo Transitorio. De acuerdo con este mismo precepto este plazo se hace extensible a los sujetos obligados del orden federal, toda vez que se establece este mismo período de seis meses para el ajuste de las disposiciones jurídicas federales.

En relación con lo anterior, el segundo párrafo del artículo Segundo Transitorio de la LGPDPPSO prevé el supuesto de que el Congreso de la Unión o las legislaturas de las entidades federativas omitan realizar las adecuaciones legislativas correspondientes dentro del plazo de los seis meses. Ante esta situación, la ley general tendrá una aplicación directa "con la posibilidad de seguir aplicando de manera supletoria las leyes preexistentes en todo aquello que no se oponga a la misma, hasta en tanto no se cumpla la condición impuesta en el presente artículo." Esta disposición se explica en el supuesto de que las entidades federativas no adecúen su propia normatividad, en cuyo caso la ley general cobra una aplicación directa, no así por lo que se refiere al ámbito federal, toda vez que el artículo 1º de la misma ya prevé dicha aplicación directa para los sujetos obligados pertenecientes al orden federal. De tal forma que, para el caso del orden federal, el sentido de esta disposición adquiere un sentido diverso, que consiste en generar un mandato para el legislador a fin de adecuar las disposiciones jurídicas federales y, con ello, ampliar el plazo de aplicación de esta ley para que éste no sea a partir de la iniciación de vigencia, plazo que, a su vez, se extiende en términos del artículo Séptimo Transitorio.

En el segundo supuesto, el artículo Séptimo Transitorio establece el plazo de dieciocho meses siguientes a la entrada en vigor de esta ley, para que los sujetos obligados puedan tramitar, expedir o modificar su normatividad interna. Como puede observarse de su texto, no se encuentra limitado a los sujetos obligados del orden federal, lo cual podría implicar, bajo una interpretación literal, que este plazo resulta aplicable, también, a los sujetos obligados del orden estatal y municipal. Cabe hacer notar que el plazo comienza a correr a partir de la entrada en vigor de la ley y no a partir de que se hayan realizado los ajustes normativos correspondientes, tanto a nivel federal como estatal. El hecho de que esta disposición sólo haga referencia a la emisión de la normatividad interna por parte de los sujetos obligados, abre las puertas a serias disquisiciones sobre si este plazo (dieciocho meses) resulta extensible

[327] Véase el artículo 1 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

al cumplimiento de los principios, deberes y procedimientos que establece la ley que no suponen necesariamente la emisión de normatividad interna.

En el tercer supuesto, cabe mencionar lo dispuesto por el artículo Quinto Transitorio, mismo que hace referencia al plazo de un año a partir de la entrada en vigor de la ley para que el INAI y los organismos garantes de cada entidad federativa emitan los diversos lineamientos a que se refiere la ley. Este plazo se encuentra dirigido a las facultades regulatorias o cuasi-regulatorias de los órganos garantes del derecho a la protección de datos personales. A manera de ejemplo, considérense las facultades del INAI para emitir lineamientos o para el debido tratamiento de datos personales para el ejercicio de los derechos ARCO, de conformidad con lo previsto en esta ley general en el artículo 89, fracciones XXVII y XXVIII, respectivamente. De nueva cuenta se abren espacios importantes para la interpretación, pues este artículo transitorio hace referencia, específicamente, a los "lineamientos", lo cual, en opinión de la autora, podría hacerse extensible a otras facultades referidas a la emisión de "disposiciones administrativas de carácter general".

Un cuarto supuesto corresponde al mandato expresamente dirigido al Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales para que emita el Programa Nacional de Protección de Datos Personales, de conformidad con el artículo 12 de la propia ley general. Para este caso específico, el artículo Sexto Transitorio establece el plazo de un año a partir de la entrada en vigor de esta ley.

Ahora bien, en cuanto a sus efectos, la técnica legislativa distingue entre la abrogación y derogación de otros ordenamientos o disposiciones jurídicas. La primera implica dejar sin efectos cualquier ley u ordenamiento jurídico en la materia y la segunda hace referencia a la privación parcial de dichos efectos.[328] De conformidad con el artículo Cuarto Transitorio de esta ley general, el legislador optó por la figura de la derogación. De tal forma que las normas jurídicas emitidas con anterioridad a la expedición de esta ley podrán subsistir y tendrán vigencia en tanto no se opongan a lo dispuesto por la propia ley. Ciertamente cada entidad federativa tiene plena libertad para determinar qué normas jurídicas propias de su jurisdicción considera que deben subsistir y cuáles no, pero siempre que sean conformes a las disposiciones de esta ley general.

Por otra parte, el artículo Tercero Transitorio establece un mandato dirigido específicamente a la Cámara de Diputados del Congreso de la Unión, así como a las legislaturas de las entidades federativas, para que adopten previsiones presupuestarias específicas para el ejercicio fiscal 2018, a fin de dar cumplimiento a lo dispuesto por esta nueva ley general, misma que, si

[328] Véase nota 326.

bien no implica la introducción de un nuevo derecho, sí contempla múltiples acciones que incrementan sustantivamente las tareas de los órganos garantes del derecho a la protección de datos personales.

Finalmente, el artículo Octavo Transitorio establece que las entidades federativas no podrán ampliar o reducir, en perjuicio de los titulares de datos personales, los procedimientos y plazos vigentes aplicables en la materia. Esto no es otra cosa que la positivización del principio pro persona para el desarrollo normativo en cada estado de la República Mexicana.

## IV. Conclusiones

Los artículos transitorios previstos en la LGPDPPSO adoptan el contenido general que suele distinguirlos, esto es, especifica el plazo para su iniciación de vigencia, los plazos que deberán seguirse para su aplicación y exigibilidad, así como diversos mandatos dirigidos a los órganos garantes del derecho a la protección de datos personales, al Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, a los sujetos obligados en los diversos órdenes de gobierno y órganos legislativos encargados de su ajuste y armonización. De igual forma establece, de manera específica, la necesidad de contar con previsiones presupuestarias que permitan su operatividad. En ese sentido, todos ellos cumplen con el carácter provisional propio de los artículos transitorios. No obstante, algunos de ellos son susceptibles de interpretación ante la ausencia de precisión en cuanto a su alcance y contenido.

## Referencias

DOF. (1928). Código Civil Federal, *Diario Oficial de la Federación*.

DOF. (2017). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, *Diario Oficial de la Federación*.

Huerta, K. (2001). Artículos Transitorios y Derogación, *Boletín Mexicano de Derecho Comparado*, núm. 102, septiembre-diciembre. México: Instituto de Investigaciones Jurídicas de la UNAM, pp. 811-840.

López, M. (2000). “Técnica legislativa y proyectos de ley”, en Carbonell, M. y Pedroza de la Llave, S. (Coords.), *Elementos de Técnica Legislativa*. México: UNAM. [Archivo PDF]. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/1/21/tc.pdf, [fecha de consulta: 8 de mayo 2018].

Muro, E. (2007). *Algunos Elementos de Técnica Legislativa*. México: Instituto de Investigaciones Jurídicas de la UNAM. [Archivo PDF]. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/5/2149/2.pdf, [fecha de consulta: 8 de mayo 2018].

Segundo Tribunal Colegiado en materia Administrativa del Sexto Circuito. (octubre 2001). Tesis VI.2o.A.1K, Novena Época, *Semanario Judicial de la Federación y su Gaceta*. Tomo XIV, p. 1086.

**LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS, COMENTADA,**

Edición a cargo de:
Dirección General de Comunicación Social y Difusión.
Dirección General de Promoción y Vinculación con la Sociedad.

inai

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales