EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN MÉXICO. NUEVOS RETOS PARA LA ADMINISTRACIÓN PÚBLICA

THE RIGHT TO THE PROTECTION OF PERSONAL DATA IN MEXICO. NEW CHALLENGES FOR THE PUBLIC ADMINISTRATION

María Amparo Ramírez Necoechea[1]

Resumen

En México el reconocimiento del derecho a la protección de datos personales es posterior a países europeos; además, tuvo un surgimiento legal y posteriormente constitucional. Su importancia radica en que a nivel internacional es considerado un derecho humano desde el año 2000. Este trabajo tiene como objetivo analizar el derecho a la protección de datos personales en México en el contexto tecnológico, retomando su origen, reconocimiento, desarrollo y consolidación como derecho autónomo para, posteriormente, plantear las acciones del poder Ejecutivo y detectar los retos que enfrenta la administración pública mexicana respecto de la ejecución normativa. La estrategia metodológica utilizada es documental y se basa en el desarrollo legal y constitucional del derecho a la protección de datos personales en México, por lo que los datos utilizados son de carácter cualitativo. El resultado de la investigación es el reconocimiento del largo camino recorrido, del gran alcance obtenido al lograr la homologación normativa en todo el territorio nacional, pero también la detección de las implicaciones y los desafíos que enfrenta la administración pública en México a partir de la emisión, en enero de 2017, de la Ley General de Protección de Datos Personales.

Palabras clave: protección de datos personales, derecho a la protección de datos personales, derecho humano a la protección de datos personales

1 Doctora en Administración Pública, Maestra en Derecho Constitucional y Amparo, Licenciada en Derecho. Actualmente cursa el Doctorado en Ciencias de Gobierno y Política en la Benemérita Universidad Autónoma de Puebla. México. Correo: maría.ramireznecoechea@viep.com.mx

Abstract
In Mexico, the recognition of the right to protection of personal data is later than European countries, furthermore, it had a legal and later constitutional emergence. Its importance lies in the fact that at an international level it has been considered a human right since 2000. This work aims to analyze the right to the protection of personal data in Mexico in the technological context, returning to its origin, recognition, development and consolidation as a right autonomous, to subsequently propose the actions of the executive branch and detect the challenges faced by the Mexican Public Administration, regarding regulatory execution. The methodological strategy used is documentary and is based on the legal and constitutional development of the right to the protection of personal data in Mexico, so the data used is qualitative in nature. The result of the research is the recognition of the long path traveled, the great scope obtained by achieving regulatory approval throughout the national territory, but also the detection of the implications and challenges faced by the Public Administration in Mexico from the issuance, in January 2017, of the GZeneral Law on Protection of Personal Data.
Key words: Protection of personal data, right to protection of personal data, human right to the protection of personal data

Introducción

Los datos personales se refieren a la información de una persona física, identificada o identificable, como el origen étnico o racial, las características físicas, morales o emocionales, de la vida afectiva y familiar, el domicilio, patrimonio, ideología, creencias, estados de salud, preferencias sexuales, u otras que afecten su intimidad (Ornelas y López Ayllón, 2010, p. 64).

El derecho a la protección de datos personales emergió en el contexto de la transmisión masiva de información, que significó la necesidad de resguardar los datos más íntimos de las personas. La protección de datos personales en México derivó en gran parte de recomendaciones de organismos e instrumentos internacionales vinculantes.

Actualmente México cuenta con varias leyes de protección de datos personales; una Ley Federal cuya aplicabilidad es en el sector privado, una Ley General que tiene aplicabilidad para el sector público en los tres niveles: federal, estatal y municipal. Además, 32 leyes estatales que se encuentran homologadas a la Ley General.

Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados se encuentra vigente desde 2017 y establece las mínimas garantías para que cada estado de la República Mexicana se apegue a ésta, pudiendo ampliar los mecanismos de protección en cada caso. El problema detectado radica precisamente en la ejecución de la Ley General y de las Leyes Estatales homologadas, principalmente debido a los requerimientos tecnológicos que se exigen, entre otros retos.

El objetivo de esta investigación es realizar un análisis legal del derecho a la protección de datos personales en México en el contexto tecnológico, retomando su origen, desarrollo e impulso, y detectar algunos desafíos latentes dentro de la administración pública mexicana como ejecutora y garante de este derecho humano.

La estructura del presente trabajo versará en cuatro apartados. En el primer apartado se describirá el contexto en el que surge la protección de datos personales, considerando sus antecedentes normativos europeos derivados del avance de la tecnología. En el segundo apartado se analizará el surgimiento legal y la posterior inclusión constitucional en México. En el tercer apartado se analizará la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados. Finalmente, en el cuarto apartado se expondrán los retos que la administración pública enfrenta en el contexto digital y las conclusiones.

1. Antecedentes normativos y contexto

1.1. Origen europeo y su clasificación legislativa

El derecho a la protección de datos personales tiene un origen europeo (Piñar Mañas, 2003, p. 39). El surgimiento de esta legislación puede clasificarse en leyes de primera, segunda tercera y cuarta generación.

Las Leyes de Primera Generación comprenden desde 1970 a 1973 y se caracterizan por la escasez de desarrollo de la informática (Puente Escobar, 2006, p. 40). La primera Ley surgió en Alemania, en *Land de Hesse*, el 7 de octubre de 1970 (Téllez, 2002, pp. 28-58); era breve y exclusivamente protegía los datos informáticos susceptibles de tratamiento por organismos públicos (Garriga, 1999, pp. 48-49).

La Resolución 509 de la Asamblea del Consejo de Europa, sobre los derechos humanos y los nuevos logros científicos y técnicos, impulsó las recomendaciones de 1973, para evitar mal empleo de la información, posteriormente se emiten las directrices para la creación de bancos de datos en el sector público y comenzaron a desarrollarse leyes. La primera Ley Nacional sobre Protección de Datos por el Parlamento Sueco de 1973. Es el texto de referencia, pues extiende su aplicación al sector público y al privado. Desarrolla por primera vez los principios que lo configuran y crea la primera autoridad en materia de protección de datos.

Las Leyes de Segunda Generación comprenden desde 1974 hasta 1979, e inician con la *Privacy Act* estadounidense, que protege a individuos frente al asalto a la intimidad por los sistemas de acopio y almacenamiento de datos derivados del uso de tecnología informática por agencias federales y bancos de datos (Pérez Luño, 1989, p. 147). La Ley francesa de 1978 relativa a Informática, ficheros y libertades, define los datos personales y prevé un órgano específico y de estructura colegiada para velar por su aplicación y recibir quejas de las personas afectadas. Entre 1977 y 1979, Alemania, Dinamarca, Austria y Luxemburgo adoptan leyes nacionales de protección de datos de carácter personal, guiadas por el marco de la ley sueca de 1973 y creando autoridades independientes (Puente Escobar, 2006, p. 41). De manera simultánea, la Protección de Datos Personales se incorporó a textos fundamentales. Portugal, en 1976, fue el primero en incluir este derecho en su Carta Magna. El Artículo 35 refiere "1. Todos los ciudadanos tienen derecho a acceder a los datos informatizados, pudiendo exigir su rectificación y actualización, así como conocer la finalidad". Asimismo, en la Constitución Española de 1978 el Artículo 18.4 dice: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos".

Las Leyes de Tercera Generación comprenden desde 1980 hasta 2000, e inician con el reconocimiento internacional de las facultades jurídicas que surgen a partir de la libertad informática. Los documentos internacionales más importantes son: las directrices de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre circulación internacional de datos personales para la protección de la intimidad, de 1980; el Convenio 108 del Consejo de Europa para la protección de las personas respecto del tratamiento automatizado de sus datos de carácter personal, de 1981; y, la Directiva 95/46/CE relativa a la protección de datos personales y a la libre circulación de estos de 1995, actualmente derogada por el Reglamento General de Protección de Datos.

Las Leyes de Cuarta Generación surgen finalmente con la proclamación de la Carta de Derechos Fundamentales de la Unión Europea, del año 2000, donde el derecho a la protección de datos personales ya es considerado un Derecho Humano.

1.2. Consolidación como derecho autónomo

En un inicio estuvo íntimamente ligado al derecho a la privacidad; sin embargo, en virtud de que el desarrollo tecnológico ha redimensionado las relaciones del ser humano y su marco de convivencia, el Derecho a la Intimidad ha alcanzado nuevos matices hasta llegar al Derecho de Protección de Datos Personales, como un derecho independiente. Autores como Ricard Martínez (2004, p. 47), Martí Capitanachi (2007, p. 104), Carpizo (2003, p. 237) y Estadella (1995, p. 32) conceptualizan ambos derechos y los diferencian. Por su parte, Pérez Luño (1996, p. 319), lo considera una mera extensión del derecho a la intimidad.

La privacidad es un ámbito de la vida que se tiene derecho a proteger de cualquier intromisión, es la parte más profunda de la vida de una persona, comprende sus sentimientos, vida familiar, relaciones de amistad e inclusive gustos y pasatiempos. El artículo 12 de la Declaración Universal de los Derechos Humanos dicta: "Nadie será objeto de injerencias arbitrarias en su vida privada".

Méjan (1996, p. 69) precisa que la intimidad es el derecho a mantener en reserva situaciones de la vida privada, ya sean circunstancias, experiencias, sentimientos o conductas que el ser humano prefiere manterner para sí mismo, y este derecho debe ser reconocido y resguardado por el sistema jurídico.

Las tecnologías de la información han tenido una gran influencia en el concepto de privacidad, introducido desde el clásico *The Right of Privacy*, de 1890, la intimidad como disciplina jurídica ha perdido su carácter individual y privado, para asumir progresivamente una significación pública y colectiva (García González, 2007, p. 15).

El derecho a la intimidad es el derecho a ser dejado solo y evitar injerencias en la vida privada mientras que el derecho a la protección de datos atribuye a la persona un poder de disposición y control sobre los datos que le conciernen, y que son objeto de tratamiento público y privado.

Davara (2005, p. 47), Murillo (1990, p. 120), Herrán Ortiz (1999, p. 89) y Piñar Mañas (2006, p. 32) han descrito a la protección de datos personales como el conjunto de intereses que pueden ser afectados por la elaboración de informaciones referentes a personas identificadas o identificables. Además, es la facultad de participar en el tratamiento

que otros hacen de sus datos personales y proteger el manejo justo de su información, a través de los derechos ARCO; es decir, del derecho a acceder, rectificar, cancelar u oponerse al tratamiento de los datos personales. El Derecho a la Protección de Datos Personales protege la información personal en general; no solo la más íntima, otorgando la facultad de controlar el uso, destino y permanencia en bases de datos.

1.3. Reconocimiento como derecho humano

El Artículo 8 la de Carta de Derechos Fundamentales de la Unión Europea, firmada en Niza el 7 de diciembre de 2000, establece: "1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

Los derechos humanos se basan en la dignidad humana y destacan la calidad de las personas e impulsan lograr dentro de la sociedad su realización como seres humanos. Son el conjunto de facultades, prerrogativas, libertades y pretensiones de carácter civil, político, económico, social y cultural que se le reconocen al ser humano (Ángeles, 2012, p. 172; Garzón, 1993, p. 531); Puy, 2009, p. 50; Nogueira, 2009, p. 11).

La Primera Generación relativa a los derechos civiles y políticos, surgió en el siglo XVIII. Únicamente se consideraban a los derechos o libertades individuales, que consistían en la autolimitación y la no injerencia de los poderes públicos en la esfera privada de las personas. La Revolución Francesa detonó su reconocimiento, los derechos obtenidos derivaron de la expresión de libertad de los individuos frente al Estado. Ejemplo se estos derechos son: la personalidad jurídica, la vida, la integridad física y moral, la libertad personal, la libertad de expresión, la libertad de asociación, el debido proceso, el honor, la nacionalidad, la seguridad y la privacidad.

La Segunda Generación es el paquete de derechos reconocidos en el Pacto Internacional de Derechos Económicos, Sociales y Culturales de la Asamblea General de Las Naciones Unidas, en 1976. Se refieren a la existencia de condiciones de vida y de acceso a los bienes materiales y culturales por la dignidad inherente. Surgen con la Revolución Industrial y las luchas sociales del siglo XIX. Se exige la intervención del Estado

para garantizar el acceso a derechos y compensar desigualdades de clases. Se obliga al Estado a crear tribunales y procedimientos para dirimir controversias entre particulares y aplicar la ley a quienes hayan dejado de observarla. Derecho a la salud y a la educación y los derechos denominados de participación, representaron una obligación de hacer para el Estado y para satisfacer necesidades sociales a través de servicios.

La Tercera Generación emerge con las Tecnologías de la Información y Comunicación (TIC). Algunos derechos se deterioraron y otros nuevos surgen. Tal es el caso de la paz social, la calidad de vida, el derecho a la libertad informática y a la protección de datos personales (Pérez Luño, 2006, p. 28; Javier de Lucas, 1993, p. 19).

Estos derechos de tercera generación se caracterizan por aparecer en el contexto del Derecho Internacional Humanitario, que persigue preservar la vida, la dignidad y la salud de las víctimas de guerras. Son también denominados *los derechos colectivos de la humanidad*, pues emergen a partir de la Segunda Guerra Mundial. Ejemplos se estos derechos son: el derecho a la paz, solidaridad, desarrollo y a un medio ambiente sano.

Algunos autores consideran que la tercera generación únicamente se refiere al reconocimiento de derechos en grupos sociales y que existe una cuarta generación relativa al reconocimiento de los derechos de la sociedad digital. Al respecto, Ortega Martínez (2004, p. 664) refiere que los de cuarta generación se sustentan en la necesidad inédita de asegurar a todos los individuos el acceso a las tecnologías de información y comunicación, fomentar el flujo e intercambio de información, alentando la transferencia de conocimientos y estimulando la formación de capital humano.

Tercera o cuarta generación, la diferencia entre ambas generaciones radica en conjuntar el desarrollo de las TIC con el surgimiento de ciertas prerrogativas a partir del derecho humanitario; sin embargo, lo que es destacable es el hecho de que la era digital marcó una coyuntura en términos de derechos humanos. Surgen nuevos derechos que tienen por objetivo proteger un nuevo estatus del individuo en la sociedad digital. Además, nuevos derechos humanos buscan proteger la vida privada y la igualdad en las condiciones de acceso a las TIC. Se requiere la participación de todos los actores sociales; el ciudadano, el Estado, las entidades públicas y privadas y la comunidad internacional, incorporando el valor fundamental de la solidaridad.

2. Surgimiento legal en México e inclusión constitucional

2.1. Surgimiento legal en México

El camino hacia la protección de los datos personales en México se impulsó con la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, de 2002, que estableció que los datos personales se consideran información confidencial. Tenía aplicabilidad para el poder Ejecutivo federal y excluía del ámbito competencial del incipiente órgano garante a los otros poderes y a los órganos constitucionales autónomos.

A pesar de su breve mención a la protección de datos personales, la Ley ya establecía los deberes de los sujetos obligados para recabar y tratar los datos personales, así como para permitir el ejercicio de los Derechos de Acceso y Rectificación, sin incluir Cancelación y Oposición. Establecía los principios, derechos, la existencia de un registro de protección de datos, así como las algunas reglas en torno a los procedimientos de acceso y corrección de datos personales.

2.2. Reconocimiento Constitucional en México

Al inicio, la Constitución mexicana solo contemplaba a la privacidad, junto con el conocido principio de legalidad. Artículo 16 Constitucional: "nadie puede ser molestado en su persona, familia, domicilio, papeles, posesiones; pudiendo llevarse esta molestia solamente mediante el mandato de una autoridad competente".

El 20 de julio de 2007 fue publicada en el *Diario Oficial de la Federación* (*DOF*), la reforma al Artículo 6 de la Constitución, adicionando 7 fracciones al segundo párrafo, con el objetivo de homologar el Derecho de Acceso a la Información Pública Gubernamental en cualquier punto del territorio nacional y para los tres niveles de gobierno en México:

> Artículo 6.- […] Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases: […] II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes […] III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso

> gratuito a la información pública, a sus datos personales o a la rectificación de éstos.

Con ello se amplió el ámbito de aplicación a los poderes ejecutivo, legislativo y judicial tanto federal como estatal, pues la Ley Federal de Transparencia únicamente era vinculante para el poder Ejecutivo federal.

En 2008 se inició un proceso constitucional para crear un derecho independiente y dotar a los mexicanos de un poder de disposición sobre sus datos personales. El 1 de junio de 2009 se publicó la reforma al Artículo 16 de la Constitución adicionando un segundo párrafo:

> Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.
> 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.

El 30 de abril de 2009, a través de la reforma al Artículo 73, se concedieron facultades al Congreso de la Unión para legislar en materia de protección de datos personales en posesión de particulares, con lo que quedó subsanada la insuficiencia del Artículo 6. Así, el 5 de julio de 2010 se publicó la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en el *DOF* y su Reglamento el 21 de diciembre de 2011.

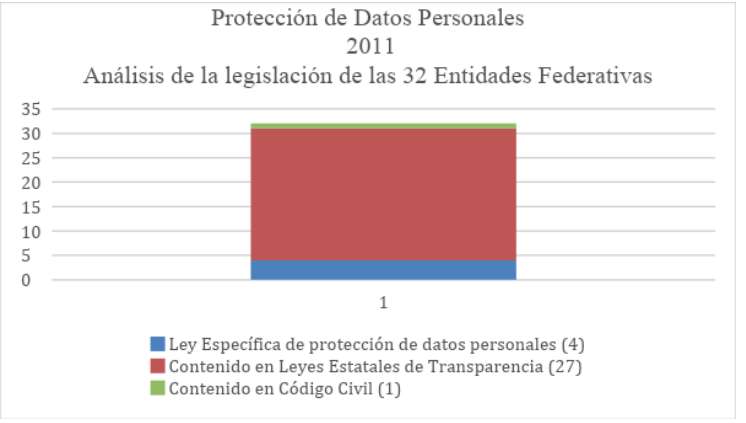
Posteriormente, el 10 de junio de 2011 se publicó en el *DOF* la Reforma Constitucional en materia de Derechos Humanos. Respecto de la protección de datos personales implicó que aquellos tratamientos de datos personales que tengan como efecto una violación a los derechos humanos; tales como el derecho a la privacidad, el derecho a la no discriminación y el derecho de asociación, podrían ser inconstitucionales o inconvencionales.

3. Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados: antecedentes, contenido y aspectos relevantes

3.1. Antecedentes

Las nuevas disposiciones constitucionales ampliaron el ámbito competencial a los tres niveles de gobierno estatales y federales. A partir de la publicación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares del 2010, los estados comienzan a publicar leyes específicas o a incluirlo en leyes de transparencia. Además, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental rige al sector público y la ley de 2010 es exclusiva para el sector privado.

En 2011 Óscar Guerra Ford realizó un estudio comparativo de las legislaciones existentes en México en el ámbito local y federal; el cual conluyó que únicamente cuatro entidades: Colima, Distrito Federal, Guanajuato y Oaxaca cuentan con leyes específicas en materia de protección de datos personales. Jalisco incorpora la normatividad en su Código Civil y su Ley de Transparencia; y los 27 estados restantes incluyen la protección de datos personales en sus leyes de Transparencia (2011, pp. 110-126).



Fuente: elaboración propia.

La dispersión normativa, la emisión de las Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana, diversos estudios, recomendaciones en foros internacionales, y por disposiciones normativas nacionales e internacionales el 7 de febrero de

2014, se publicó en el *DOF* el Decreto por el que se reforman y adicionan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos en materia de transparencia y protección de datos personales.

Los aspectos relevantes de la reforma fueron principalmente la transformación de la naturaleza jurídica del Instituto Federal de Acceso a la Información Pública y de sus homólogos estatales, dotándolos de autonomía constitucional; la legitimación a los órganos garantes, para promover acciones de inconstitucionalidad; y la ampliación de los sujetos obligados incluyendo a los poderes Ejecutivo, Legislativo 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.

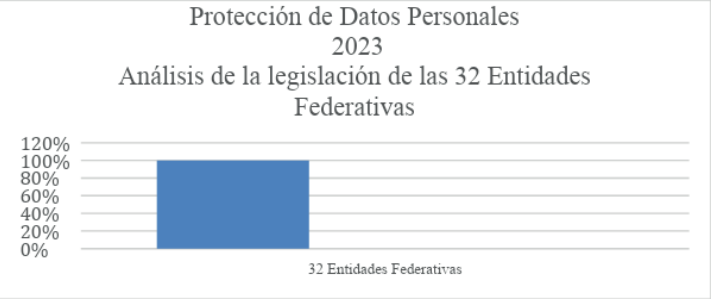
Así también, destacó la obligación de establecer procedimientos de revisión expeditos que se sustanciarán ante los organismos autónomos especializados. Además, estableció la facultad de atracción para conocer, de oficio o a petición fundada del organismo garante de los recursos de revisión trascendentes. También incluyó que las resoluciones del órgano constitucional autónomo serán vinculatorias, definitivas e inatacables; no obstante, se faculta al Consejero Jurídico del gobierno para interponer recurso de revisión ante la Suprema Corte de Justicia de la Nación cuando peligre la seguridad nacional.

La reforma incluye también la obligación de todas las autoridades y servidores públicos para coadyuvar con el órgano constitucional autónomo. Finalmente, faculta al Congreso de la Unión para emitir una Ley General que establezca las bases, principios generales y procedimientos del ejercicio del derecho a la protección de datos personales en todos los niveles de gobierno. La Ley General fue publicada el 26 de enero de 2017 y entró en vigor el 27 de enero del mismo año.

El artículo segundo transitorio de la Ley General, establece el plazo de seis meses a partir de la entrada en vigor para que las Entidades Federativas ajusten sus disposiciones normativas o emitan una nueva ley homologada en un plazo de seis meses. De las 32 Entidades, 23 cumplieron en tiempo y 9 lo hicieron con posterioridad, el plazo venció el 27 de julio de 2017.

Fuente: elaboración propia.

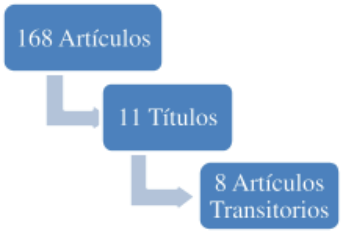
Como resultado de la emisión de la Ley General, actualmente se tiene cubierta la protección de los datos personales en los tres niveles de gobierno del sector público. Además, cada entidad federativa posee una legislación específica y homologada en los estándares mínimos señalados por la Ley General. Claramente hay un avance normativo en comparación con el análisis de 2011, donde únicamente 4 entidades contaban con dicha legislación.



Fuente: elaboración propia.

Aspectos de la Ley General relativos a la designación de autoridades específicas, órganos garantes, obligaciones definidas y procedimientos de revisión e inconformidad, son de avanzada en comparación con otros países. Contreras (2022, p. 3) plantea que en el caso de Chile hay una deficiente recepción del derecho a la protección de datos personales en la Constitución, junto a una legislación precaria y obsoleta que contribuye a su desconocimiento y desprotección. También hay ausencia de una

autoridad de control y se debe recurrir a los Tribunales de Justicia y a la práctica jurisprudencial, especialmente a nivel de acciones de protección.



3.2. Contenido de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados

Objetivos:
Distribuir competencias entre los Organismos Garantes.
Establecer las bases mínimas y condiciones homogéneas del tratamiento de los datos personales y del ejercicio de los derechos ARCO.
Regular la organización y operación del Sistema Nacional de Transparencia.
Garantizar la observancia de los principios de protección de datos personales.
Proteger los datos personales en posesión de cualquier autoridad, entidad, órgano y organismo de los tres niveles, de los tres poderes y órganos autónomos, partidos políticos, fideicomisos y fondos públicos.
Garantizar que toda persona pueda ejercer este derecho.
Promover, fomentar y difundir una cultura de protección de datos personales.
Garantizar el cumplimiento a través de mecanismos y de medidas de apremio.
Regular los medios de impugnación y procedimientos para la interposición de acciones de inconstitucionalidad y controversias constitucionales.

Disposiciones generales:

El Capítulo I contiene el objeto de la ley de establecer bases, principios y procedimientos para garantizar este derecho. Establece quiénes son sujetos obligados, en el ámbito federal, estatal y municipal. También contiene definiciones.

El Capítulo II se refiere al Sistema Nacional de Transparencia y su función de coordinar acciones y establecer e implementar criterios y lineamientos.

Principios y deberes:

Explica los principios de licitud, finalidad, lealtad, consentimiento, calidad, proporcionalidad, información y responsabilidad en el tratamiento de datos personales. Establece el deber de mantener las medidas de seguridad con independencia del tipo de sistema en el que se encuentren los datos personales.

Derechos de los titulares y su ejercicio:

El Capítulo I expone los derechos de Acceso, Rectificación, Cancelación y Oposición. Acceder y conocer la información relacionada con las condiciones de su tratamiento. Rectificar o corregirlos cuando resulten inexactos, incompletos o no actualizados. Cancelar los archivos, registros, expedientes y sistemas, para que dejen de ser tratados. Oponerse al tratamiento cuando aun siendo lícito debe cesar para evitar un daño o perjuicio al titular, o dejen de ser objeto de tratamiento automatizado.

El Capítulo II contiene los procedimientos y plazos para el ejercicio de los Derechos ARCO.

El Capítulo III se refiere a la Portabilidad de los Datos y contempla que cuando se traten datos personales por vía electrónica en un formato estructurado, el titular tendrá derecho a obtener del responsable una copia en un formato electrónico que le permita seguir utilizándolos.

Relación del responsable y el encargado:

Su único capítulo dispone que el encargado deberá realizar las actividades de tratamiento sin poder de decisión sobre el alcance y contenido del mismo y que la relación entre el responsable y el encargado deberá estar formalizada mediante contrato o instrumento jurídico.

De las comunicaciones de datos personales:

Su único capítulo hace referencia a las características de las Transferencias.

Acciones preventivas en materia de protección de datos personales:

El Capítulo I contempla que se deberán impulsar mejores prácticas.

El Capítulo II se refiere a las Bases de Datos en Posesión de Instancias de Seguridad, Procuración y Administración de Justicia.

Responsables en materia de protección de datos personales:

El Capítulo I contiene disposiciones relativas al Comité de Transparencia el cual será la autoridad máxima y funcionará conforme a lo dispuesto en la Ley General de Transparencia.

El Capítulo II dispone que cada Sujeto Obligado deberá contar con una Unidad de Transparencia que deberá auxiliar al titular en relación con el ejercicio de los derechos ARCO, también funcionará conforme a lo dispuesto en la Ley General de Transparencia y Acceso a la Información Pública.

Organismos garantes:

El Capítulo I es el relativo al Institito Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales y contiene sus funciones principales.

El Capítulo II establece las funciones, atribuciones y deberes de los órganos garantes.

El Capítulo III instituye la coordinación entre los órganos garantes y la promoción del derecho a la Protección de Datos Personales.

Procedimientos de impugnación:

El Capítulo I contiene disposiciones generales de los Recursos de Revisión y de Inconformidad.

El Capítulo II describe los procedimientos, términos y plazos del Recurso de Revisión.

El Capítulo III describe los procedimientos, términos y plazos del Recurso de Inconformidad.

El Capítulo IV es el relativo a la Atracción de los Recursos de Revisión trascendentes.

El Capítulo V El Consejero Jurídico del Gobierno Federal podrá interponer recurso de revisión en materia de seguridad nacional ante la Suprena Corte de Justicia de la Nación.

El Capítulo VI Una vez que hayan causado ejecutoria las resoluciones el Instituto podrá emitir los criterios de interpretación pertinentes y que deriven de lo resuelto.

Facultad de verificación del Instituto y los organismos garantes:

El Capítulo Único El Instituto y los Organismos garantes, de oficio o por denuncia, tendrán la atribución de vigilar y verificar el cumplimiento de las disposiciones de la Ley.

Medidas de apremio y responsabilidades:

El Capítulo I las medidas de apremio podrán ser amonestación pública, o multa, equivalente a la cantidad de ciento cincuenta hasta mil quinientas veces el valor diario de la Unidad de Medida.

El Capítulo II se refiere a las Sanciones y establece que las de carácter económico no podrán ser cubiertas con recursos públicos.

3.3. Aspectos técnicos relevantes

Dentro de las disposiciones contenidas en la ley, se detectaron tres tareas complejas que implican recursos tecnológicos.

La creación de sistemas de datos personales.

En el mejor de los casos se cuenta con algunos expedientes físicos desorganizados o algunas bases de datos que difícilmente sirven para proporcionar a la ciudadanía el ejercicio de los derechos ARCO. Es necesario digitalizar expedientes y crear sistemas de datos personales por cada finalidad o propósito para el que se recaben. La ley estipula, por lo menos los siguientes:

a) De los integrantes del sujeto obligado: quienes laboran en las dependencias y entidades, contenidos en los expedientes laborales.

b) De los proveedores: personas físicos o morales contratadas para prestar algún servicio.

c) De aquéllos que realicen trámites y servicios; es decir, se refiere a la creación de Sistemas por cada uno de los trámites y servicios que se presten.

En este apartado surge el cuestionamiento de ¿cómo determinar cuántos sistemas de datos personales debe tener cada sujeto obligado?, la respuesta depende de cada finalidad para que los ocupe y esto está ligada con cada una de las competencias establecidas en sus normatividades.

La asignación de los niveles de seguridad

Para ello es necesario previamente la clasificación de los datos personales al generar los Sistemas de Datos Personales. La ley contempla 3 niveles de seguridad: bajo, medio y alto. En el nivel de seguridad bajo entran todos los datos personales. El nivel medio aplica para datos concernientes a infracciones administrativas, hacienda pública, servicios financieros, datos patrimoniales, así como datos de carácter personal que permitan obtener una evaluación de la personalidad del individuo. El nivel de seguridad alto será para los datos sensibles. Los criterios de clasificación de datos personales son subjetivos, principalmente en lo referente a los datos personales sensibles. Al no existir un listado específico de categorías, es posible que no se protejan apropiadamente.

La implementación de las medidas de seguridad.

Se trata de garantizar la confidencialidad, integridad y disponibilidad de los datos personales y que los responsables lleven a cabo un manejo cuidadoso de los datos personales (Artículo 32.) Pueden ser administrativas, físicas o técnicas.

1.- Las medidas administrativas son para:

a) La gestión, soporte y revisión de la seguridad de la información a nivel organizacional.

b) La identificación, clasificación y borrado de la información.

2.- Las medidas físicas son para:

a) Prevenir el acceso no autorizado a la organización, instalaciones, recursos e información.

b) Prevenir daño o interferencia a instalaciones, áreas críticas, recursos e información.

c) Proteger dentro y fuera recursos móviles, portátiles, soportes físicos o electrónicos.

d) Proveer a equipos que almacenan datos personales de mantenimiento eficaz.

3.- Las medidas técnicas son para:

a) Asegurar que el acceso a las bases de datos sea por usuarios autorizados.

b) Generar privilegios o perfiles de acceso a los datos en función de las atribuciones.

c) Prevenir el daño o interferencia a las instalaciones, recursos e información.

d) Revisar la configuración de seguridad del software y hardware.

e) Gestionar las comunicaciones, operaciones y medios de almacenamiento de los recursos informáticos en el tratamiento de datos personales.

Adicionalmente, la Ley prevé que se deberán:

a) Establecer medidas especiales en función de ciertos factores-riesgo, su sensibilidad, el desarrollo tecnológico, las transferencias y las vulneraciones a la seguridad ya ocurridas.

b) Implementar un sistema de gestión de seguridad; elementos y actividades interrelacionadas para establecer, revisar y mejorar el tratamiento y seguridad.

c) Elaborar un documento de seguridad que describa los elementos indispensables que permitirán asegurar un cuidado adecuado de los datos personales.

Es importante precisar el tratamiento de datos personales, también se encuentra contemplado en otras normatividades. Tanto la Ley General de Transparencia y Acceso a la información Pública

como la Ley General de Archivos, consideran un sistema en el que se desarrollan medidas de interoperabilidad institicional para la gestión documental, implementación de documentos electrónicos, digitalización, intermediación de datos, conexión a red, entre otros aspectos que requieren de tecnologías para su operación y cumplimiento. Diversa legislación converge y tiene relación intrínseca en todo momento con la protección de datos personales, también la relativa a los medios de comunicación y a los derechos humanos en general por lo que se demandan estudios multidisciplinares (Hernández, 2021, p. 6).

4. Problemas de ejecución de la norma y otros retos relacionados con el contexto digital

Tras el análisis de las disposiciones normativas, se detectan algunas disposiciones que por su naturaleza pueden considerarse obstáculos en alguna etapa, estos se relacionan con el desarrollo tecnológico escaso en el país y los problemas de brecha digital y conectividad latentes en México. Así también los relativos a la transmisión masiva de información de carácter personal y las invasiones a la privacidad que en aras de seguridad pueden ocasionarse.

4.1. Aprovechar las Tecnologías de la Información y la Comunicación

Las TIC facilitan el almacenamiento de la información pero también, facilitan la proliferación de información. Los datos personales circulan en la red de forma masiva, por lo que es necesario la regulación, control y protección de la información.

El desafío de las TIC impacta directamente en la recolección, procesamiento y transmisión de datos personales, pues para garantizar los derechos ARCO e implementar lo que la Ley establece en cuanto las medidas de seguridad y clasificación, se requieren crear bases de datos en formatos electrónicos, digitalizar expedientes físicos, contar con portales virtuales y controlar la transmisión de los datos.

Con el desarrollo de las TIC existen constantes violaciones a la privacidad de las personas, accesos, usos y transmisiones indiscriminadas y no autorizadas de información personal, estos fenómenos también se hacen presentes en los archivos gubernamentales. Hasta la utilización masiva de la informática para el tratamiento de datos no se producía una intromisión tan importante y agresiva en la esfera personal e íntima de las personas (Parra, 2011, p. 177). Esta intromisión es una amenaza

desconocida que implica el reconocimiento de un derecho y la necesidad de nuevos mecanismos de protección (Davara, 2014, p. 9).

Incluso con la inteligencia artificial, nuevos cuestionamientos predominan respecto de violaciones de otros derechos; tal es el caso de los derecho de autor. Además se han puesto en discusión elementos de análisis para determinar si el desarrollo de tencología están propiciando ambientes de vulneración de ciberseguridad y con ello robo de datos y de identidad. Especial protección requieren los datos sensibles, como los datos biométricos; sin embargo, parecen los más vulnerables ante el impulso de tecnologías de última generación como la inteligencia artificial.

Paradójicamente, las TIC han complicado el proteger más y mejor el derecho a la protección de datos personales de los ciudadanos. A pesar de ello, también han facilitado el otorgamiento de trámites y servicios en línea. Esto plantea nuevos retos, como la necesidad de autenticación por medios electrónicos sin la presencia física simultánea de las partes, así como, de manera prioritaria la debida protección de datos personales. Es la posibilidad de gestionar la administración de manera eficiente lo que nos lleva a la necesidad de tomar en consideración que la información, sea personal o no, deja de ser un bien para convertirse en un servicio (Ornelas y Alcalde, 2014, p. 14).

La administración pública enfrenta constantemente el reto de modernizar las plataformas, medios y sistemas para la captura y resguardo de los datos personales, pues con los avances tecnológicos hacen cada vez menos práctico y seguro la utilización de papel, pero siempre a través de la creación de sistemas electrónicos adecuados y en apego a lo que establece la ley.

Parra Noriega (2011, p. 149) destaca la importancia de la protección de datos personales en la administración pública, ya que para atender sus funciones públicas, la autoridad, requiere contar con bases de datos de sus gobernados. La posesión de datos personales conlleva un riesgo importante para los titulares de los datos, quienes se ven amenazados a ser objetivos de su uso indebido.

Se trata de avances tecnológicos en beneficio de las personas, siempre y cuando se garanticen sus derechos, tales como la propiedad intelectual, el derecho a la información o a la libertad de expresión. Estos avances tecnológicos hacen que las actividades gubernamentales, educativas, sociales y económicas sean más sencillas, accesibles y eficientes; sin embargo, de manera paralela representan riesgos potenciales derivados del uso excesivo, inadecuado e irresponsable (Ornelas y Alcalde, 2014, p. 17).

4.2. Garantizar el pleno ejercicio de los derechos ARCO en un contexto digital

Cada persona debe conocer quién tratará sus datos personales, para qué finalidad; si se podrá ceder o permitir el acceso a terceros, y los casos en que la información debe ser objeto de publicidad. Todo tratamiento de datos personales debe sujetarse a mediadas de seguridad y confidencialidad. Los datos sometidos a tratamiento deben ser utilizados en el marco del respeto a la dignidad de la persona y a su poder de disposición sobre ellos. Es necesario que en la recopilación y tratamiento de datos se observen los principios que garanticen la seguridad en el manejo de los mismos.

El uso indebido de los datos personales puede tener consecuencias graves para una persona, que pueden ir desde la provocación de actos de molestia al titular de los datos, consistente en el envío ilimitado de información no solicitada, pasando por actos de discriminación, o la construcción de perfiles que pueden influir negativamente al momento de solicitar un servicio o adquiera un bien, hasta la comisión de delitos graves, como secuestro o robo de identidad.

4.3. Ejecutar las disposiciones normativas de la materia

Para la administración pública el principal reto es la correcta aplicación de la ley y la ejecución de cada una de las disposiciones y acciones que establece la nueva normatividad, que no solo garantiza la protección de los datos personales bajo su resguardo sino el correcto ejercicio de los derechos ARCO.

Para el cumplimiento de sus funciones y objetivos la administración pública recaba información confidencial, como lo son los datos personales. Cada Sujeto Obligado debe crear los Sistemas de Datos Personales por cada finalidad o propósito por el que se recaben. Este es uno de los principales desafíos. Sistemas de Datos Personales: conjunto organizado de datos personales en posesión de los entes públicos, contenidos en archivos, registros, ficheros, bases o bancos de datos, clasificados de manera que se pueda acceder a ellos en cualquiera que fuere la modalidad de su creación o almacenamiento.

La Ley General establece el registro de los Sistemas en la Plataforma Nacional de Transparencia. Continúan los problemas en la identificación de sistemas de datos personales, confusión sobre el origen, competencia, atribución y resguardo de los datos personales contenidos en los sistemas; dudas en la identificación de datos personales y las categorías de estos; y dificultad sobre el contenido, finalidad, uso y destino de los sistemas de datos personales así como la clasificación para otorgar el nivel

de seguridad. A pesar de que los niveles de seguridad y tecnología por implementar que establece la legislación en concreto son muy avanzados, existen otras propuestas y mecanismos para aumentar la seguridad en la protección de datos personales (Recio, 2014, p. 41).

Para evitar vulneración que pueda comprometer la seguridad de los datos se deben agregar acciones y controles específicos de carácter administrativo, físico y técnico. Estas acciones se refieren, entre otras, a la gestión y resguardo de soportes físicos y electrónicos, el uso de bitácoras para el registro de accesos y operaciones cotidianas, la gestión de incidentes, el plan de contingencia, la capacitación del personal y la construcción de una cultura institucional de seguridad integral (Ornelas y Alcalde, 2011, pp. 217-235).

Estos desafíos se reflejan claramente en los resultados de la evaluación realizada por el Instituto Nacional de Transparencia y Acceso a la Información Pública (INAI, 2023), del 3 de octubre de 2022 al 28 de febrero de 2023. Esta primera evaluación diagnóstica del desempeño de los sujetos obligados se centró en el cumplimiento de la Ley General. Se llevó a cabo a nivel federal y consistió en una revisión virtual de los apartados de protección de datos personales de los portales de internet de todos los sujetos obligados del padrón. Se valoró el cumplimiento de 43 criterios relativos a principios, deberes, ejercicio de los derechos ARCO, portabilidad, acciones preventivas y responsables en materia de protección de datos personales[2].

Se evaluó a los 635 sujetos obligados del padrón. Los resultados arrojaron que 118 sujetos obligados, equivalente al 18.54%, no cuentan con apartado virtual de protección de datos personales dentro de sus sitios de internet. Por lo tanto, casi el 20% incumple esta disposición normativa relativa a la creación de apartados virtuales que permitan presentar información y facilitar el ejercicio de los derechos ARCO.

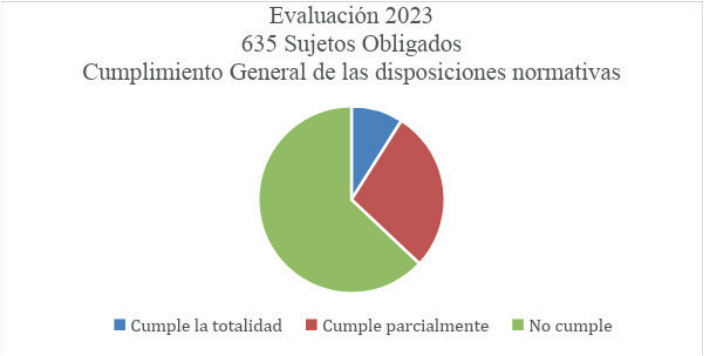
2 Disponible en: https://home.inai.org.mx/wp-content/documentos/pdp/estadisticas/evaluaciondesemp/informe_resultados_evaluacion_%202022-2023.pdf

Fuente: elaboración propia.

De los 517 que sí cuentan con apartado virtual, 237 ya publican total o parcialmente información y medios de verificación; sin embargo 280, equivalente al 54.16%, no cuentan con información. Los resultados muetran que más de la mitad de los sujetos obligados evaluados, a pesar de contar con un apartado virtual, no publican la información ni tienen los medios idóneos para cumplir a cabalidad las disposiciones normativas y permitir el ejercicio del derecho a la protección de datos personales. Una de las obligaciones incumplidas es que no están publicando los avisos de privacidad integrales.

Fuente: elaboración propia.

El cumplimiento general señaló que de los 635 solo el 9% tiene un cumplimiento igual a 100%, el 28% cumplimiento menor a 100% y el 63% tiene un cumplimiento nulo.



Fuente: elaboración propia.

A seis años de la publicación de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, esta evaluación realizada por el INAI a los 635 Sujetos Obligados Federales, arroja de manera general que un 63% está incumpliendo la normatividad totalmente, las razones van desde la complejidad de disposiciones hasta los aspectos tecnológicos como la creación de apartados virtuales en los portales de internet; y sin duda, la elaboración de las bases de datos, y la clasificación de los niveles de seguridad pertinentes continúa siendo un aspecto importante por considerar.

El INAI debe acompañar a los sujetos obligados para garantizar que se protejan los datos personales de los ciudadanos. El 27 de enero de 2024 se cumplen 7 años de la entrada en vigor de la Ley General y únicamente el 9% de los sujetos obligados evaluados cumplen las disposiciones legales al 100%.

Conclusiones

Este nuevo derecho encontró su fundamento como consecuencia de las trasformaciones sociales y culturales de la sociedad y a las nuevas formas de comunicación de los seres humanos. Su reconocimiento internacional como Derecho Humano en el año 2000, significó un impulso mundial que generó la emisión de normas específicas o el perfeccionamiento de legislación existente.

Las crecientes amenazas tecnológicas, ocasionaron que se otorgaran garantías constitucionales a todo individuo para hacer frente al uso y control de sus datos personales. Las TIC generaron el surgimiento de nuevos derechos para proteger la privacidad y la intimidad, que

posteriormente tuvieron mayor alcance al consolidar un nuevo derecho autónomo e independiente que prevé el ejercicio de los derechos ARCO.

Esto implicó la necesidad de que la administración pública continuara con el proceso de digitalización iniciado durante el periodo neoliberal[3], con la implementación del gobierno electrónico al comenzar a digitalizar documentos para otorgar trámites en línea.

En el contexto de la revolución tecnológica, el gobierno electrónico y el surgimiento de nuevos derechos humanos derivados de la transmisión de información, surge el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, que tiene por objetivo garantizar los derechos de acceso a la información pública y protección de datos personales.

Ha sido un largo camino para consolidar este derecho en México, desde su surgimiento legal en 2002, como excepción al derecho de acceso a la información pública, hasta su inclusión constitucional en 2007, derivado del reconocimiento como derecho humano en el año 2000.

Tres han sido las más impretantes reformas constitucionales que han permitido reconocer la autonomía de este derecho, 2007, 2009 y 2014, ésta última la que mayor impacto tuvo al estipular la creación de la Ley General que no solo terminó con la dispersión normativa existente, sino que estableción parámetros tecnológicos y de seguridad con estándares internacionales.

El análisis de la Ley General permitió detectar tres aspectos técnicos relevantes y complejos que implican tecnología: creación de sistemas de datos para cada finalidad que sean recabados, clasificación para asignación de niveles de seguridad y la implementación de las medidas de seguridad. Así también se determinaron los siguientes desafíos para la administración pública en el contexto digital:

1.- Aprovechar las Tecnologías de la Información y la Comunicación (TIC).

2.- Garantizar el pleno ejercicio de los derechos ARCO.

3 La crisis fiscal de los años ochenta obligó a una reestructuración financiera y administrativa del Estado con el fin de restablecer sus funciones sociales constitucionales. La reestructuración *neoliberal* obligó a realizar varias reformas interdependientes e implicó descentralización, privatizaciones, disminusión del aparato gubernamental, la reforma fiscal, la liberación de mercados y la implementación de la Nueva Gestión Pública o transformación gerencial que compactó niveles jerárquicoa, elevó el valor de la eficacia económica, se enfocó en la calidad, privilegió las subcontrataciones, el servicio profesional de carrera y las evaluaciones de desempeño; y puso en marcha al gobierno electrónico (Aguilar, 2013, p. 284).

> 3.- Ejecutar las disposiciones normativas de la materia (creación de bases de datos, clasificación de información, niveles de seguridad, datos sensibles, etc.).

Con el análisis de las implicaciones de la Ley General, con la exposisicón de los resultados de la evaluación realizada por el INAI en 2023, respecto del cumplimiento de las disposiciones contenidas en la Ley General por parte de los sujetos obligados, se muestra que incluso con una buena normatividad es muy arduo otorgar un buen resguardo de los datos personales pues, a pesar de que la mayoría de sus consideraciones ya se encuentran previstas por la ley de la materia, el implementarlas y ejecutarlas resulta una tarea compleja.

Es importante destacar que dentro de los datos personales existe una subclasificación relativa a los datos sensibles que requiere mayores medidas de seguridad y protección. Las medidas deben extremarse en caso de datos sensibles o si el tratamiento permite delimitar un perfil claro de la situación más íntima de las personas, ya sea una situación familiar o económica. Tal es el caso de las bases de datos relacionadas con programas sociales o relativas a subsidios, ya que a partir del conocimiento de estos datos se pueden obtener conclusiones demasiado específicas, ocasionando mayor vulnerabilidad.

Actualmente, en la era digital, es necesario continuar con la creación de bases de datos y sistemas de datos personales con las medidas de seguridad previstas por la normatividad aplicable que ha tomado en cuenta la normatividad internacional. La digitalización es inminente, pero requiere del uso responsable de la tecnología y cumplir con la legislación correspondiente en todo momento.

Garantizar derechos digitales implica procurar que los ciudadanos tengan capacidad de uso de la tecnología y preservar los derechos de los individuos frente a la tecnología. Pero una garantía efectiva de los derechos en la era digital impone obligaciones a los poderes públicos para posibilitar un acceso pleno a las herramientas tecnológicas que permita el desarrollo de su personalidad en el mundo digital contemporáneo (Rallo, 2020, p. 31).

Referencias bibliográficas

Aced Felez, E. (2000). Transacciones electrónicas en Internet. En Jornadas sobre protección de la privacidad. Telecomunicaciones e Internet. Pamplona, 22 y 23 de junio de 2000. Pamplona, Navarra, España: Agencia de protección de datos y Universidad Pública de Navarra.

Ángeles Cerón, E. (2012). El Consejo Consultivo del Estado de Hidalgo y el ejercicio de los derechos humanos. En Sexto Congreso Nacional de Organismos Públicos Autónomos: Autonomía, universidades y medios de comunicación: una visión integral en la difusión de los derechos fundamentales. Llevado a cabo en Mérida, Yucatán, , México, en 2011. Comisión de Derechos Humanos del Distrito Federal.

Carpizo, J. (2011). Los Derechos Humanos: Naturaleza, Denominación y Características. *Revista Mexicana del Derecho Constitucional*, (25), julio-diciembre. México: UNAM, Instituto de Investigaciones Jurídicas.

Contreras, P. (2022). *¿Una segunda oportunidad?* Protección de datos personales y autodeterminación informativa en una nueva Constitución chilena. *Revista Brasileira de Políticas Públicas*, *12*, agosto, 128-151.

Davara Fernández de Marcos, I. (2010). Protección de Datos de Carácter Personal en México: problemática jurídica y estatus normativo actual. En *Protección de Datos Personales Compendio de Lecturas y Legislación*. México: Tiro Corto Editores.

Davara Fernández de Marcos, I. (2014). *El derecho al olvido en relación con el derecho a la protección de datos personales*. En colección de ensayos para la transparencia de la ciudad de México, ensayo 23. México: Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal.

De Lucas, J. (1993). *El concepto de solidaridad*. México: Fontamara.

Denninger, E. (1987). El derecho a la autodeterminación informativa. En *Problemas Actuales de la Documentación y la Informática Jurídica* (traducción de Pérez Luño). Madrid, España: Tecnos.

Estadella Yuste, O. (1995). *La protección de la intimidad frente a la transmisión internacional de datos personales*. Madrid, España: Tecnos.

García González, A. (2006). La protección de datos personales dentro del ámbito judicial en México. *AR. Revista de Derecho Informático*, (101), diciembre. México.

Garriga Domínguez, A. (1999). *La protección de los datos personales en el derecho español*. Madrid, España: Dykinson.

Garzón Valdés, E. (1993). *Derecho, ética y política*. Madrid, España: CEC.

Gratton, P. (1998). *Protección informática*. México: Trillas.

Guerra Ford, Ó. (2011). Las legislaciones de protección de datos personales

en el país. En *Retos de la protección de datos personales en el sector público*. México: Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal.

Hernández Gómez, S. (2021). Alternativas de investigación em los estudios de comunicación: El acceso a la información pública y su privacidad como derecho humano en México. Revista *Dilemas Contemporáneos: Educación, Política y Valores*, 2 de octubre de 2021.

Herrán Ortiz, A. I. (1999). *La Violación de la Intimidad en la Protección de Datos Personales*. Madrid, España: Dykinson.

Martí Capitanachi, L. y Córdoba del Valle, E. (coordinadores) (2007). *Colección Transformaciones Jurídicas en el contexto de la globalización. Volumen I*. Universidad Veracruzana. Veracruz, México: Arana y CONACYT.

Méjan, L. M. C. (1996). *El derecho a la intimidad y la informática*. México: Porrúa.

Nogueira Alcalá, H. (2009). *La interpretación constitucional de los derechos humanos*. Lima, Perú: Ediciones Legales.

Ortega Martínez, J. (2004). *Sociedad de la Información y derechos humanos de la cuarta generación. Un desafío inmediato para el derecho constitucional*, en Derecho Constitucional. Memoria del Congreso Internacional de Culturas y Sistemas Jurídicos Comparados. Miguel Carbonell, coordinador. México: Universidad Nacional Autónoma de México.

Ornelas Núñez, L. y Alcalde Urbina, S. (2011). La seguridad como una pieza clave en el rompecabezas de la protección de datos personales. En *Retos de la Protección de Datos Personales en el Sector Público*. México: Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal.

Ornelas Núñez, L. y Alcalde Urbina, S. (2014). *La protección de datos personales de menores en la era digital*. En colección de ensayos para la transparencia de la ciudad de México, ensayo 24. México: Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal.

Ornelas Núñez, L. y López Ayllón, S. (2010). La recepción del Derecho a la Protección de Datos Personales en México: breve descripción de su origen y estatus legislativo. En *Protección de Datos Personales Compendio de Lecturas y Legislación*. México: Tiro Corto Editores.

Ornelas Núñez, L. y Martínez Rojas, E. (2010). Transferencias Internacionales de Datos Personales: su protección en el ámbito del comercio internacional. En *Protección de Datos Personales Compendio de Lecturas y Legislación*. México: Tiro Corto Editores.

Parra Noriega, L. G. (2011). Desarrollo legislativo en materia de datos personales en las entidades federativas, la importancia de una legislación especial en el ámbito estatal. En *Retos de la Protección de Datos Personales en el Sector Público*. México: Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal.

Pérez Luño, A. E. (1984). *Derechos humanos, Estado de derecho y Constitución*. Madrid, España: Tecnos.

Pérez Luño, A. E. (2004). *Los derechos fundamentales*. Madrid, España: Tecnos.

Pérez Luño, A. E. (1996). Perfiles morales y políticos del derecho a la intimidad. En *Anuales de la Real Academia de las Ciencias Morales y Políticas*, año XLVIII, (73). Madrid, España.

Pérez Luño, A. E. (2006). *La tercera generación de derechos humanos*. Navarra, España: Aranzadi.

Piñar Mañas, J. L. (2006). *La Red Iberoamericana de Protección de Datos (Declaraciones y Documentos)*. Valencia, España: Tirant lo Blanch.

Piñar Mañas, J. L. y Ornelas Núñez, L. (2013*). La Protección de Datos Personales en México*. México: Tirant lo Blanch.

Puy Muñoz, F. (1985). *Derechos humanos. Vol. 2. Derechos civiles*. Santiago de Compostela, España: Paredes.

Puy Muñoz, F. (2009). *Teoría Tópica de los Derechos Humanos*. Madrid, España: Colex.

Puente Escobar, A. (2006). Breve descripción de la evolución histórica y del marco normativo internacional del derecho fundamental a la protección de datos de carácter personal. En *II Encuentro Iberoamericano de Protección de Datos. La Antigua- Guatemala, 2-6 de junio de 2003* (2ª edición). Valencia, España: Tirant lo Blanch.

Rallo Lombarte, A. (2020). Una nueva generación de derechos digitales. *Revista de Estudios Políticos*, enero.

Rebollo Delgado, L. (2005). *El derecho fundamental a la intimidad* (2ª edición). Madrid, España: Dikinson.

Recio Gayo, M. (2014). *La protección de datos en el ámbito de las telecomunicaciones e internet*. En colección de ensayos para la transparencia de la Ciudad de México, ensayo 25, México: Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal.

Uvalle Berrones, R. (1997). *Las transformaciones del Estado y la Administración Pública en la sociedad Contemporánea*. México: Universidad Autónoma del Estado de México e Instituto de Administración Pública del Estado de México.

Documentos internacionales

Declaración Universal de los Derechos Humanos. Recuperado de: https://www.un.org/es/about-us/universal-declaration-of-human-rights.

Carta de Derechos Fundamentales de la Unión Europea, Niza, 2000. Recuperado de: https://www.europarl.europa.eu/charter/pdf/text_es.pdf.

Directrices sobre circulación internacional de datos personales para la protección de la intimidad, 1980 OCDE. Recuperado de: https://www.oecd.org/sti/ieconomy/15590267.pdf.

Convenio 108 del Consejo de Europa para la protección de las personas respecto del tratamiento automatizado de sus datos de carácter personal. Estrasburgo, Francia, 1981. Recuperado de: https://rm.coe.int/1680078b37.

Directiva 95/46/CE del Parlamento Europeo y del Consejo de Europa relativa a la protección de datos personales a la libre circulación de estos, 1995. Recuperado de: https://www.oas.org/es/sla/ddi/docs/Directiva-95-46-CE.pdf.

Legislación mexicana

Constitución Política de los Estados Unidos Mexicanos. Recuperado de: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

Reforma Constitucional al artículo 6, publicada en el *DOF* el 20 de julio de 2007.

Reforma Constitucional al artículo 16, publicada en el *DOF* el 1 de junio de 2009.

Reforma Constitucional al artículo 73, publicada en el *DOF* el 30 de abril de 2009.

Reforma Constitucional en materia de derechos humanos, publicada en el *DOF* el 10 de junio de 2011.

Reforma Constitucinal en materia de transparencia y protección de datos personales, publicada en el *DOF* el 7 de febrero de 2014.

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, 2002. Recuperado de: https://www.diputados.gob.mx/LeyesBiblio/abro/lftaipg/LFTAIPG_orig_11jun02.pdf.

Ley Fedral de Transparencia y Acceso a la Información Pública, 2016. Recuperado de: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP.pdf.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 2010. Recuperado de: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf.

Ley General de Transparencia y Acceso a la Información Pública, 2015. Recuperado de: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP.pdf.

Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados, 2017. Recuperado de: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf.

Ley General de Archivos, última reforma, enero de 2023. Recuperado de: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGA.pdf.

Otros documentos

INAI (2023). Informe de resultados de la evaluación del desempeño de los sujetos obligados en el cumplimiento de las disposiciones en materia de protección de datos personales 2022-2023. Emitido por la Secretaría de Protección de Datos Personales del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Recuperado de: https://home.inai.org.mx/wp-content/documentos/pdp/estadisticas/evaluaciondesemp/informe_resultados_evaluacion_%202022-2023.pdf.